CA ARCserve® Central Host-Based VM Backup

Benutzerhandbuch

r16.5



CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA Technologies:

- CA ARCserve® Backup
- CA ARCserve® D2D
- CA ARCserve® Replication and High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

CA Kontaktieren

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Support-Links für CA ARCserve Central Applications:

CA Support Online stellt eine Vielfalt an Ressourcen zur Lösung von technischen Problemen zur Verfügung und bietet einfachen Zugriff auf wichtige Produktinformationen. Mit CA Support haben Sie zu jeder Zeit schnellen und einfachen Zugang zu vertrauenswürdigen Auskünften. Über die folgenden Links gelangen Sie zu den unterschiedlichen CA Support-Seiten, die Ihnen zur Verfügung stehen:

- **Informationen zum Support**: Über diesen Link erhalten Sie Informationen zu Wartungsprogrammen und Support-Angeboten sowie zu Bedingungen, Rechtsansprüchen, Service Level Objectives (SLO) und Servicezeiten.

  https://support.ca.com/prodinfo/centappssupportofferings

- **Registrierung für Support**: Dieser Link führt Sie zum CA Support Online-Registrierungsformular, mit dem Sie Ihren Produkt-Support aktivieren können.

  https://support.ca.com/prodinfo/supportregistration

- **Technischer Support**: Die folgende Verknüpfung führt Sie zur One-Stop Product Support-Seite für CA ARCserve Central Applications.

  https://support.ca.com/prodinfo/arccentapps

Änderungen in der Dokumentation

Seit der letzten Version von CA ARCserve Central Host-Based VM Backup wurden folgende Aktualisierungen der Dokumentation vorgenommen:

- Das Dokument wurde mit Benutzer-Feedback, Verbesserungen, Korrekturen und anderen kleineren Änderungen aktualisiert, um die Verwendung und das Produktverständnis oder die Dokumentation selbst zu verbessern.
- Der Abschnitt Erstellen von Sicherungsrichtlinien (siehe Seite 79) wurde aktualisiert. Dieses Thema schließt zwei neue Optionen auf der Registerkarte "Sicherungseinstellungen/Erweitert" ein: "Speicherplatz auf Ziel reservieren" und "Katalog". Außerdem wurden auf der Registerkarte "Voreinstellungen/E-Mail-Alerts" zwei Alerts zu Zusammenführungsjobs hinzugefügt und eine Fehlermeldung entfernt.
- Der Abschnitt Bearbeiten oder Kopieren von Sicherungsrichtlinien (siehe Seite 83) wurde aktualisiert. Dieses Thema schließt jetzt zwei neue Optionen auf der Registerkarte "Sicherungseinstellungen/Erweitert" ein: "Speicherplatz auf Ziel reservieren" und "Katalog".
- Der Abschnitt Anzeigen von CA ARCserve Central Host-Based VM Backup-Protokollen (siehe Seite 91) wurde aktualisiert. Dieses Thema schließt jetzt zwei neue Optionen in der Drop-down-Liste "Module" ein: "Mehrere Knoten aktualisieren" und "CA ARCserve D2D-Zusammenführungsjob".
- Der Abschnitt Wiederherstellen eines gesamten virtuellen Rechners (siehe Seite 108) wurde aktualisiert. Dieses Thema wurde aktualisiert, um das aktuelle Design des Dialogfelds widerzuspiegeln.
- Der Abschnitt Zugriffsverweigerungsfehler beim Aktualisieren von Knoten (siehe Seite 134) wurde aktualisiert. Dieses Thema schließt jetzt zwei Lösungen für das Deaktivieren der Benutzerkontensteuerung (UAC) ein.
- Der Abschnitt Durchführen einer Bare-Metal-Recovery (siehe Seite 167) wurde aktualisiert. Dieses Thema schließt nun das neue Hilfsprogramm zum Erstellen eines WinPE-ISO für BMR ein (Bootkit für Bare Metal Recovery erstellen). ISO-Dateien werden nicht mehr zur Verfügung gestellt. Zusätzlich unterstützt dieser Abschnitt BMR von Sicherungen, die auf UEFI-Rechnern durchgeführt wurden, auf BIOS-Rechnern und von Sicherungen, die auf BIOS-Rechnern durchgeführt wurden, auf UEFI-Rechnern.
- Der Abschnitt So erstellen Sie ein Bootkit (siehe Seite 187) wurde hinzugefügt. Dieses Thema wurde hinzugefügt, um die neue Funktionalität und die Funktionen des neuen Hilfsprogramms für die Erstellung von einzuschließen, um WinPE-ISO-Images für BMR einzuschließen.

  Hinweis: "Erstellen des Bootkits"wurde entfernt und durch dieses Thema ersetzt.

- Der Abschnitt zur Anwendungswiederherstellung von Microsoft Exchange Server wurde mit neuen Szenariothemen zu So stellen Sie Microsoft Exchange-Anwendungen wieder her aktualisiert. Dieses Thema schließt jetzt Exchange 2013 Support ein, siehe die Informationen zu Voraussetzungen und Überlegungen zur Wiederherstellung.
- Der Abschnitt CA ARCserve Central Host-Based VM Backup erkennt die Volumes auf den dynamischen Festplatten nicht, wenn der virtuelle Rechner auf einem alternativen ESX-Server oder Hyper-V-Server wiederhergestellt wird (siehe Seite 164) wurde hinzugefügt. Dieses Thema beschreibt die Lösung, um die Volumes auf den dynamischen Festplatten abzurufen.
- Das Thema Ausschließen von Dateien vom Antivirusscanning (siehe Seite 208) wurde hinzugefügt. Dieses Thema beschreibt die vom Antivirusscanning auszuschließenden Dateien, Ordner und Prozesse.
- Der Abschnitt über mitgelieferte Anmeldeinformationen bzw. Anmeldeinformationen des Domänenadministrators zur Anmeldung beim Gastbetriebssystem des virtuellen Rechners wurde aktualisiert.
  - Erforderliche Installationsaufgaben (siehe Seite 17)
  - Lösungen für Preflight-Check-Elemente (siehe Seite 64)
  - Zugriffsverweigerungsfehler beim Aktualisieren von Knoten (siehe Seite 134)

Inhalt

Kapitel 1: Einführung in CA ARCserve Central Host-Based VM Backup

Dieses Kapitel enthält folgende Themen:

Einführung

CA ARCserve Central Applications verbindet wichtige Datenschutz- und -Managementtechnologien mit einem Ökosystem von Zielanwendungen, die im Einklang miteinander funktionieren, um sowohl Innen- und Außenschutz als auch das Kopieren, Verschieben und Transformieren von Daten quer durch globale Umgebungen zu ermöglichen.

CA ARCserve Central Applications sind einfach zu verwenden, handzuhaben und zu installieren. Sie bieten Organisationen eine automatische Kontrolle über ihre Informationen, um fundierte Entscheidungen über den Zugriff, die Verfügbarkeit und Sicherheit ihrer Daten auf der Basis des allgemeinen Geschäftswerts zu treffen.

Informationen zu CA ARCserve Central Host-Based VM Backup

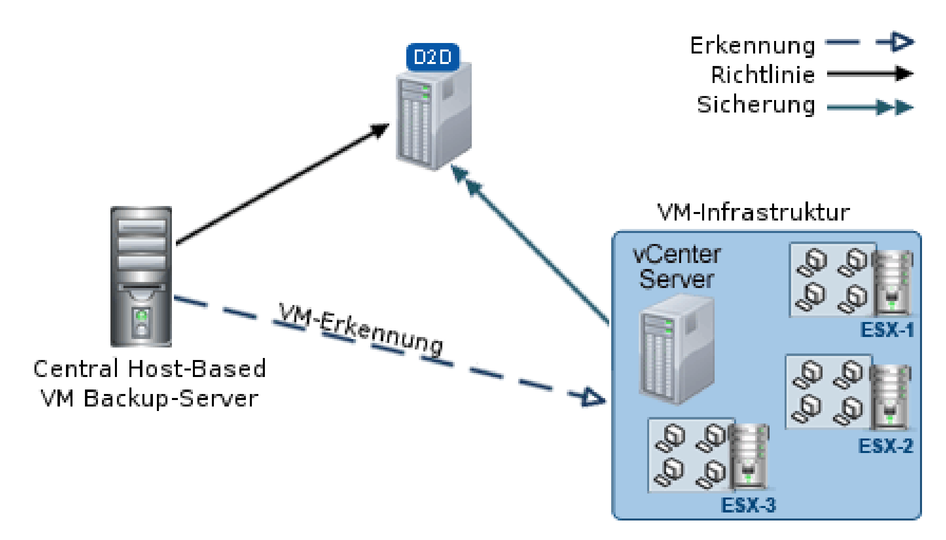
Eine der CA ARCserve Central Applications ist die Anwendung "CA ARCserve Central Host-Based VM Backup". Diese Anwendung funktioniert mit der schlanken CA ARCserve D2D-Sicherheitslösung und ermöglicht es Ihnen, mehrere virtuelle Rechner zu schützen, ohne die Software bzw. die Agenten jeweils einzeln auf den VMs installieren zu müssen. Diese Funktion minimiert die negativen Folgen mehrerer Sicherungen auf demselben physischen Server und lässt Sie auf der Grundlage Ihrer VM-Sicherungen Sicherungen auf Dateiebene, auf Anwendungsebene oder Bare-Metal-Recoverys (BMR) durchführen.

CA ARCserve Central Host-Based VM Backup ist einfach skalierbar,sodass Sie virtuelle Rechner nach Bedarf hinzufügen können, ohne zusätzliche Lizenzen erwerben oder auf jedem virtuellen Rechner in Ihrer Produktionsumgebung Software installieren zu müssen.

Funktionsweise von CA ARCserve Central Host-Based VM Backup

CA ARCserve Central Host-Based VM Backup ermöglicht es Ihnen, virtuelle Rechner auf einem ESX- oder vCenter-Server in einem einzigen Schritt zu schützen, indem eine auf einem Proxy installierte Instanz von CA ARCserve D2D verwendet wird. Verwenden Sie dafür folgende Checkliste:

1. Installieren Sie CA ARCserve D2D auf einem physischen oder virtuellen Rechner, der als ein Sicherungs-Proxy in Ihrer Umgebung fungiert. Weitere Installationsanweisungen finden Sie im Abschnitt Installieren von CA ARCserve D2D im CA ARCserve D2D-Benutzerhandbuch. Stellen Sie sicher, dass der Proxy richtig konfiguriert ist.
2. Zu verwaltende Knoten hinzufügen. Geben Sie einen ESX-Server an. Die Anwendung erkennt die auf ihm ausgeführten virtuellen Rechner, die den Anforderungen entsprechen.
3. Sicherungsrichtlinien erstellen. Geben Sie in jeder Richtlinie den Sicherungs-Proxy an, auf dem Sie CA ARCserve D2D installiert haben.
4. Weisen Sie jeder VM Sicherungsrichtlinien zu, sodass Sie alle VMs mit der einzelnen CA ARCserve D2D-Instanz schützen können, die auf dem Sicherungs-Proxy ausgeführt wird.
5. Erstellen Sie Knotengruppen, um Ihre virtuelle Rechnerumgebung besser zu verwalten. Zum Beispiel können Sie Knoten nach Geschäftsfunktion oder nach installierten Anwendungen gruppieren und anschließend eine Richtlinie zuweisen, die konfiguriert wurde, um Knoten, die einer bestimmten Funktion zugeordnet sind oder die eine bestimmte Anwendung ausführen, zu schützen.



CA ARCserve Central Applications-Bookshelf

Die Inhalte dieser CA ARCserve Central Applications-Hilfe sind auch als Benutzerhandbuch im PDF-Format verfügbar. Auf die neueste PDF-Version dieses Handbuchs und der Hilfe kann vom CA ARCserve Central Applications-Bookshelf aus zugegriffen werden.

Die Dateien mit CA ARCserve Central Applications-Versionshinweisen enthalten Informationen bezüglich Systemanforderungen, unterstützte Betriebssysteme, Support bei der Wiederherstellung der Anwendung und andere Informationen, die Sie kennen sollten, bevor Sie dieses Produkt installieren. Außerdem enthalten die Versionshinweise eine Liste bekannter Probleme, derer Sie sich bewusst sein sollten, bevor Sie CA ARCserve Central Applications verwenden. Auf die aktuelle Version der Versionshinweise kann vom CA ARCserve Central Applications-Bookshelf aus zugegriffen werden.

Kapitel 2: Installieren und Konfigurieren von CA ARCserve Central Host-Based VM Backup

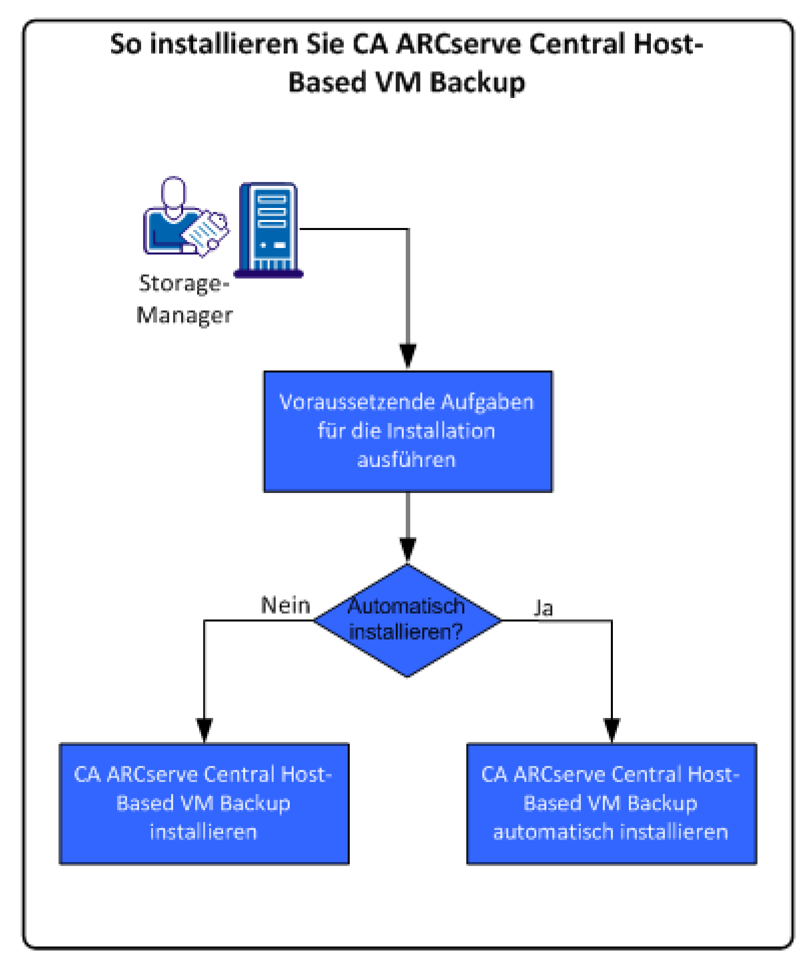
Dieses Kapitel enthält folgende Themen:

So installieren Sie CA ARCserve Central Host-Based VM Backup

Dieses Szenario beschreibt, wie Speichermanager CA ARCserve Central Host-Based VM Backup mithilfe der folgenden Methoden installieren können:

- Standardmäßige Installation: Bei dieser Methode wird ein Installationsassistent verwendet, um die Anwendung zu installieren.
- Automatische Installation: Diese Methode lässt Sie eine unbeaufsichtigte Installation unter Verwendung der Windows-Befehlszeile ausführen.

Das folgende Diagramm veranschaulicht, wie Sie die Anwendung installieren:



Die folgende Tabelle führt die Abschnitte auf, in denen die Aufgaben für die Installation von CA ARCserve Central Host-Based VM Backup beschrieben werden:

Aufgabe	Siehe Thema
Führen Sie erforderliche Installationsaufgaben aus und überprüfen Sie die Installationshinweise, bevor Sie die Anwendung installieren.	Erforderliche Installationsaufgaben (siehe Seite 17)
Führen Sie eine standardmäßige Installation mithilfe des Installationsassistenten aus.	Installieren von CA ARCserve Central Host-Based VM Backup (siehe Seite 19)
Führen Sie eine automatische Installation mithilfe der Windows-Befehlszeile aus.	CA ARCserve Central Host-Based VM Backup automatisch installieren (siehe Seite 21)

Weitere Informationen darüber, wie verschiedene Windows-Betriebssystem-Komponenten aktualisiert werden können, nachdem die Anwendung installiert wurde, finden Sie im Abschnitt über Best Practices im CA ARCserve Central Host-Based VM Backup-Benutzerhandbuch.

Erforderliche Installationsaufgaben

Bevor Sie die Anwendung installieren, schließen Sie die folgenden erforderlichen Aufgaben ab und überprüfen Sie die Installationshinweise:

Vorbereitende Aufgaben

- Überprüfen Sie die Versionshinweise. Die Versionshinweise enthalten eine Beschreibung der Systemanforderungen, unterstützten Betriebssysteme und eine Liste der Probleme, die in dieser Version der Anwendung bekannt sind.
- Stellen Sie sicher, ob Ihr System die Mindestanforderungen für die Hardware und Software erfüllt, die für die Installation der Anwendung erforderlich sind.
- Stellen Sie sicher, dass die Verfolgung geänderter Blöcke aktiviert werden kann und auf den virtuellen Rechnern aktiviert ist, die Sie schützen.

  Hinweis: Weitere Informationen zur Verfolgung geänderter Blöcke finden Sie im folgenden Knowlegde-Base-Dokument auf der VMware-Website:

  http://kb.vmware.com/kb/1020128
- Prüfen Sie, ob Sie über Administratorrechte oder die entsprechende Berechtigung zum Installieren von Software auf den Computern verfügen, auf denen Sie CA ARCserve Central Host-Based VM Backup installieren möchten.
- Stellen Sie sicher, dass Ihr vCenter- oder vSphere-Server über Administratorrechte für VMware und Windows verfügt. Ordnen Sie das Konto der Rolle "Global License" auf dem vCenter Server-System oder dem ESX-Server-System zu, damit VDDK-Vorgänge erfolgreich durchgeführt werden können.

- Prüfen Sie, ob Sie die Benutzernamen und Kennwörter der Computer haben, auf denen Sie die Anwendung, die Sie besitzen, installieren.
- Stellen Sie sicher, dass CA ARCserve D2D auf dem Sicherungs-Proxy-System, das die virtuellen Rechner in Ihrer Produktionsumgebung schützt, installiert ist.
- Wenn Sie möchten, dass Ihre VM-Sicherung die spezifische Wiederherstellung verwenden kann, überprüfen Sie, dass die mitgelieferten Anmeldeinformationen oder die Anmeldeinformationen des Domänenadministrators von allen Benutzern mit Administratorrechten angegeben sind, um sich beim Gastbetriebssystem des virtuellen Rechners anzumelden.
- Mit CA ARCserve Central Applications können Sie CA ARCserve D2D installieren und die Vorgängerversion auf Remote-Knoten mithilfe des Bereitstellungshilfsprogramms auf die aktuelle Version aktualisieren. Um Daten auf den Remote-Knoten mit der aktuellen Version von CA ARCserve D2D zu sichern, müssen Sie die aktuelle Version der CA ARCserve D2D-Lizenzen auf den Knoten anwenden. Wenn Sie die Lizenzen nicht innerhalb von 31 Tagen nach der Installation oer der Aktualisierung auf den Knoten anwenden, kann CA ARCserve D2D nicht mehr verwendet werden.

Installationshinweise

Bevor Sie CA ARCserve Central Host-Based VM Backup installieren, überprüfen Sie folgende Installationshinweise:

- Das CA ARCserve Central Applications-Installationspaket installiert ein Modul namens "CA ARCserve Central Applications-Server". Der Server ist ein Modul, das von allen Anwendungen gemeinsam verwendet wird. Das Modul enthält den Webservice, die Binärdateien und die Konfigurationen, die die Anwendungen benötigen, um miteinander zu kommunizieren.

  Wenn Sie die Anwendung installieren, installiert das Installationspaket das CA ARCserve Central Applications-Servermodul, bevor die Produktkomponenten installiert werden. Wenn ein Patch für die Anwendung angewendet werden muss, aktualisiert der Patch das Modul, bevor er die Produktkomponenten aktualisiert.
- Nachdem CA ARCserve Central Host-Based VM Backup installiert wurde, laden Sie Version 1.11 der VMware VIX-API herunter, und installieren Sie sie auf dem Sicherungs-Proxy-System sowie auf dem Computer, der verwendet wird, um Preflight-Checks auszuführen. VMware VIX wird verwendet, um Wiederherstellungen von Sicherungen auf Dateiebene und auf Anwendungsebene auszuführen.

  Hinweis: Für VIX API 1.11 ist es erforderlich, dass alle virtuellen Rechner mit den neuesten Versionen der VMware-Tools aktualisiert wurden.
- CA ARCserve D2D installiert VMware Virtual Disk Development Kit (VDDK) auf allen Rechnern, auf denen Sie CA ARCserve D2D installieren. Sie müssen VDDK nicht herunterladen und auf Ihren Sicherungs-Proxy-Systemen installieren.

Wenn Sie eine andere VDDK-Version verwenden wollen, laden Sie VDDK herunter und installieren Sie es, und ersetzen Sie dann den Wert des unter HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D angegebenen VDDKDirectory-Registrierungseintrags durch den des Installationsordners, in dem das neue VDDK installiert wurde.

Der Standardspeicherort für VDDK lautet folgendermaßen:

- **x64-Betriebssystem:**

  `C:\Programme (x86)\VMware\VMware Virtual Disk Development Kit`

  Hinweis: Entzippen Sie die VDDK64.zip-Datei vom VDDK-Installationsverzeichnis in den VDDK64-Ordner.

  Zum Beispiel: C:\Programme (x86)\VMware\VMware Virtual Disk Development Kit\VDDK64

- **x86-Betriebssystem:**

  `C:\Programme\VMware\VMware Virtual Disk Development Kit`

- Es ist eine lokale Installation von CA ARCserve D2D erforderlich, um bestimmte Wiederherstellungsvorgänge auszuführen. Weitere Informationen finden Sie im Thema Hinweise zur Wiederherstellung (siehe Seite 114). Lizenzen für CA ARCserve D2D sind in CA ARCserve Central Host-Based VM Backup enthalten. Die Produktinstallationsdateien finden Sie bei CA Support.
- Virtuelle Kompatibilität für Partitionsgerätzuordnung wird unterstützt, die physische Kompatibilität jedoch nicht.

Installieren von CA ARCserve Central Host-Based VM Backup

Der Installationsassistent hilft Ihnen dabei, führt Sie durch den Prozess, CA ARCserve Central Applications einmal oder mehrmals zu installieren.

Hinweis: Bevor Sie die Anwendung installieren, überprüfen Sie die Datei mit den Versionshinweisen und stellen Sie sicher, dass alle in Vorbereitende Aufgaben beschriebene Aufgaben ausgeführt sind.

So installieren Sie CA ARCserve Central Host-Based VM Backup

1. Laden Sie das CA ARCserve Central Applications-Installationspaket auf den Computer herunter, auf dem Sie die Anwendung installieren möchten, und doppelklicken Sie dann auf die Setup-Datei.

   Das Installationspaket extrahiert seine Inhalte auf Ihren Computer und daraufhin öffnet sich das Dialogfeld "Erforderliche Komponenten".

2. Klicken Sie im Dialogfeld "Erforderliche Komponenten" auf "Installieren".

   Hinweis: Das Dialogfeld "Erforderliche Komponenten" wird nur angezeigt, wenn Setup die erforderlichen Komponenten nicht auf dem Zielcomputer installiert findet.

   Nachdem Setup die erforderlichen Komponenten installiert hat, öffnet sich das Dialogfeld "Lizenzvereinbarung".

3. Füllen Sie die erforderlichen Optionen auf der Lizenzvereinbarung aus, und klicken Sie auf "Weiter".

   Das Dialogfeld "Konfiguration" wird geöffnet.

4. Führen Sie auf dem Dialogfeld "Konfiguration" folgende Schritte aus:

   - **Komponenten**: Geben Sie die Anwendungen an, die Sie installieren wollen.

     Hinweis: Wenn Sie diese Anwendung mithilfe des Suite-Installationspakets installieren, können Sie mehrere Anwendungen installieren.

   - **Speicherort**: Akzeptieren Sie den Standardspeicherort für die Installation oder klicken Sie auf "Durchsuchen", um einen alternativen Installationsspeicherort anzugeben. Der Standardspeicherort lautet folgendermaßen:

     `C:\Programme\CA\ARCserve Central Applications`

   - **Festplatteninformationen**: Stellen Sie sicher, dass Ihre Festplatte über ausreichenden Speicherplatz verfügt, um die Anwendungen zu installieren.

   - **Name des Windows-Administrators**: Geben Sie den Benutzernamen des Windows-Administratorkontos unter Verwendung der folgenden Syntax an:

     `Domäne\Benutzername`

   - **Kennwort:** Geben Sie das Kennwort für das Benutzerkonto an.

   - **Portnummer angeben:** Geben Sie die Portnummer an, die Sie verwenden wollen, um mit der webbasierten Benutzeroberfläche zu kommunizieren. Als Best Practice sollten Sie die standardmäßige Portnummer akzeptieren. Die standardmäßige Portnummer lautet:

     `8015`

     Hinweis: Wenn Sie eine alternative Portnummer angeben wollen, liegen die verfügbaren Portnummern zwischen 1024 und 65535. Bevor Sie eine alternative Portnummer angeben, überprüfen Sie, ob die festgelegte Portnummer frei und zur Verwendung verfügbar ist. Setup hindert Sie daran, die Anwendung mithilfe eines Ports zu installieren, der nicht zur Verwendung verfügbar ist.

- **Für Web-Kommunikationen HTTPS verwenden:** Legen Sie die Verwendung der HTTPS-Kommunikation für Datenübertragung fest. Standardmäßig ist diese Option deaktiviert.

  Hinweis: Sichere HTTPS-Kommunikation bietet eine höhere Sicherheitsebene als HTTP-Kommunikation. HTTPS ist das empfohlene Kommunikationsprotokoll, wenn Sie in Ihrem Netzwerk vertrauliche Informationen übertragen.

- **Lassen Sie zu, dass Setup die Dienste und Programme von CA ARCserve Central Applications als Ausnahmen für die Windows Firewall registriert --**Stellen Sie sicher, dass das Kontrollkästchen neben dieser Option aktiviert ist. Firewall-Ausnahmen sind erforderlich, wenn Sie CA ARCserve Central Applications von Remote-Rechnern aus konfigurieren und verwalten möchten.

  Hinweis: Benutzer, die die Anwendung lokal verwenden, brauchen keine Firewall-Ausnahmen zu registrieren.

Klicken Sie auf "Weiter".

Nachdem der Installationsprozess abgeschlossen ist, öffnet sich das Dialogfeld "Installationsbericht".

5. Das Dialogfeld "Installationsbericht" fasst die Installation zusammen. Wenn Sie jetzt nach Aktualisierungen für die Anwendung suchen wollen, klicken Sie auf "Nach Aktualisierungen suchen" und danach auf "Fertig stellen".

Die Anwendung wird installiert.

CA ARCserve Central Host-Based VM Backup automatisch installieren

CA ARCserve Central Applications ermöglicht es Ihnen, CA ARCserve Central Host-Based VM Backup automatisch zu installieren. Bei der automatischen Installation ist kein Benutzereingriff erforderlich. Die folgenden Schritte beschreiben, wie sie die Anwendung mithilfe der Windows-Befehlszeile installieren können.

So installieren Sie CA ARCserve Central Host-Based VM Backup automatisch

1. Öffnen Sie die Windows-Befehlszeile auf dem Computer, auf dem Sie den automatischen Installationsvorgang starten wollen.
2. Laden Sie das selbstextrahierende CA ARCserve Central Applications-Installationspaket auf Ihren Computer herunter.

   Starten Sie den automatischen Installationsvorgang mithilfe der folgenden Befehlszeilen-Syntax:

```
"CA ARCserve Central Applications Setup.exe" /s /v"/q
-Path:<INSTALLATIONSVERZEICHNIS> -Port:<PORT> -U:<Benutzername> -P:<Kennwort>
-Products:<Produktliste>"
```

Verwendung:

s

Lässt Sie das ausführbare Dateipaket im automatischen Modus ausführen.

v

Lässt Sie zusätzliche Befehlszeilenoptionen angeben.

q

Lässt Sie die Anwendung im automatischen Modus installieren.

-Path:<INSTALLATIONSVERZEICHNIS>

(Optional) Lässt Sie den Zielinstallationspfad festlegen.

Beispiel:

`-Path:“C:\Programme\CA\ARCserve Central Applications”`

Hinweis: Wenn der Wert für INSTALLATIONSVERZEICHNIS ein Leerzeichen enthält, setzen Sie den Pfad zwischen umgekehrte Schrägstriche und Anführungszeichen. Zudem kann der Pfad nicht mit einem umgekehrten Schrägstrich enden.

-Port:<PORT>

(Optional) Lässt Sie die Portnummer für die Kommunikation festlegen.

Beispiel:

`-Port:8015`

-U:<Benutzername>

Lässt Sie den Benutzernamen festlegen, der verwendet werden soll, um die Anwendung zu installieren und auszuführen.

Hinweis: Der Benutzername muss ein Administratorkonto oder ein Konto mit Administratorrechten sein.

-P:<Kennwort>

Lässt Sie das Kennwort für den Benutzernamen festlegen.

-Products:<ProductList>

(Optional) Ermöglicht es Ihnen, die CA ARCserve Central Applications-Anwendungen anzugeben, die automatisch installiert werden sollen. Wenn Sie keinen Wert für dieses Argument angeben, installiert der automatische Installationsvorgang alle Komponenten der CA ARCserve Central Applications-Anwendungen.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

Alle CA ARCserve Central Applications

ALLE

Hinweis: Die folgenden Beispiele beschreiben die Syntax, die erforderlich ist, um eine, zwei, drei oder alle CA ARCserve Central Applications automatisch zu installieren:

```
-Products:CMX64
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:ALL
```

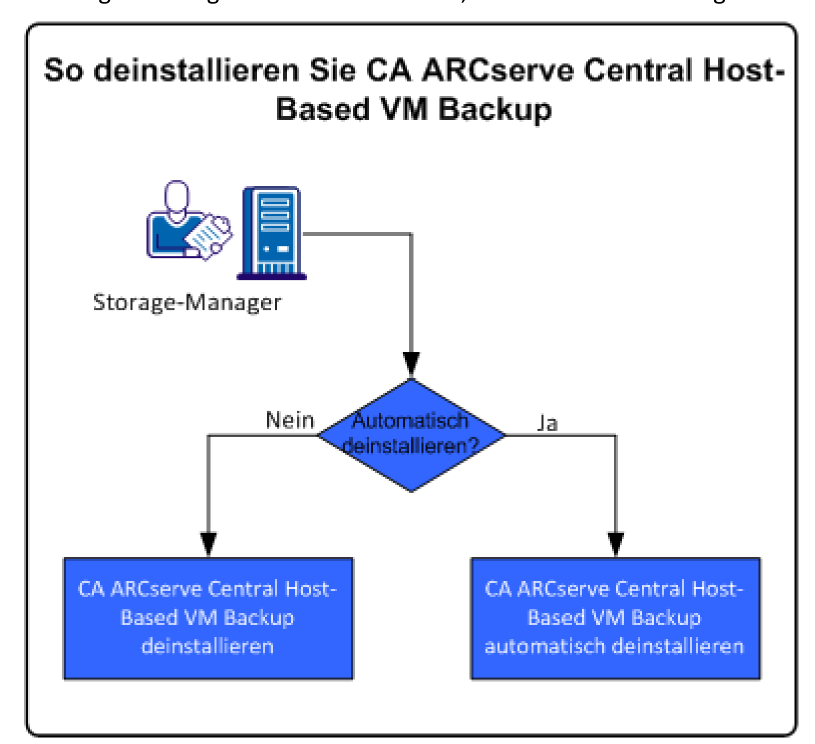
Die Anwendung wird automatisch installiert.

So deinstallieren Sie CA ARCserve Central Host-Based VM Backup.

Sie können <egvsi folgendermaßen deinstallieren:

- Standardmäßige Deinstallation: Diese Methode verwendet die Windows-Systemsteuerung, um die Anwendung zu deinstallieren.
- Automatische Deinstallation: Diese Methode lässt Sie eine unbeaufsichtigte Deinstallation unter Verwendung der Windows-Befehlszeile ausführen.

Das folgende Diagramm veranschaulicht, wie Sie die Anwendung deinstallieren:



Aufgabe	Siehe Thema
Führen Sie eine standardmäßige Deinstallation mithilfe der Windows-Systemsteuerung aus.	Deinstallieren von CA ARCserve Central Host-Based VM Backup (siehe Seite 25)
Führen Sie eine automatische Deinstallation mithilfe der Windows-Befehlszeile aus.	CA ARCserve Central Host-Based VM Backup automatisch deinstallieren (siehe Seite 26)

Weitere Informationen darüber, wie verschiedene Windows-Betriebssystem-Komponenten aktualisiert werden können, nachdem die Anwendung deinstalliert wurde, finden Sie im Abschnitt über Best Practices im CA ARCserve Central Host-Based VM Backup-Benutzerhandbuch.

Deinstallieren von CA ARCserve Central Host-Based VM Backup

Sie können die Anwendung mithilfe von Programmen und in der Windows Systemsteuerung befindlichen Funktionen deinstallieren.

So deinstallieren Sie CA ARCserve Central Host-Based VM Backup

1. Klicken Sie im Windows Startmenü auf "Start" und klicken Sie auf "Systemsteuerung".

   Die Windows Systemsteuerung wird geöffnet.

2. Klicken Sie in der Windows Systemsteuerung auf die Dropdown-Liste neben "Anzeigen" und klicken Sie danach auf "Große Symbole" oder "Kleine Symbole".

   Die Symbole für die Anwendungen der Windows Systemsteuerung werden in einer Rasteransicht angezeigt.

3. Klicken Sie auf Programme und Funktionen.

   Das Fenster "Programm deinstallieren oder ändern" öffnet sich.

4. Suchen Sie die Anwendung, die Sie deinstallieren wollen, und klicken Sie darauf.

   Klicken Sie mit der rechten Maustaste auf die Anwendung und im Pop-up-Menü auf "Deinstallieren".

   Folgen Sie den Bildschirmanweisungen, um die Anwendung zu deinstallieren.

Die Anwendung wird deinstalliert.

CA ARCserve Central Host-Based VM Backup automatisch deinstallieren

CA ARCserve Central Applications lässt Sie CA ARCserve Central Host-Based VM Backup automatisch deinstallieren. Bei der automatischen Deinstallation ist kein Benutzereingriff erforderlich. Die folgenden Schritte beschreiben, wie sie die Anwendung mithilfe der Windows-Befehlszeile deinstallieren können.

So deinstallieren Sie CA ARCserve Central Host-Based VM Backup automatisch

1. Melden Sie sich bei dem Computer an, von dem Sie die Anwendung deinstallieren möchten.

   Hinweis: Sie müssen sich über ein administratives Konto oder ein Konto mit administrativen Berechtigungen anmelden.

2. Öffnen Sie die Windows-Befehlszeile, und führen Sie folgenden Befehl aus, um den automatischen Deinstallationsvorgang zu starten:

   ```
   <INSTALLATIONSVERZEICHNIS>%\Setup\uninstall.exe /q /p <Produktcode>
   ```

   Oder

   ```
   <INSTALLATIONSVERZEICHNIS>%\Setup\uninstall.exe /q /ALL
   ```

   Beispiel: Die folgende Syntax lässt Sie CA ARCserve Central Host-Based VM Backup automatisch deinstallieren.

   ```
   "%Programme%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}
   ```

Verwendung:

<INSTALLATIONSVERZEICHNIS>

Hier können Sie das Verzeichnis angeben, in dem die Anwendung installiert ist.

Hinweis: Führen Sie die Syntax aus, die der Architektur des Betriebssystems des Computers entspricht.

<Produktcode>

Hier können Sie die Anwendung angeben, die automatisch deinstalliert werden soll.

Hinweis: Der automatische Deinstallationsvorgang lässt Sie eine oder mehrere CA ARCserve Central Applications deinstallieren. Verwenden Sie die folgenden Produktcodes, um CA ARCserve Central Applications automatisch zu deinstallieren.

CA ARCserve Central Host-Based VM Backup

{CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

CA ARCserve Central Protection Manager

{CAED05FE-D895-4FD5-B964-001928BD2D62}

CA ARCserve Central Reporting

{CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

CA ARCserve Central Virtual Standby

{CAED4835-964B-484B-A395-E2DF12E6F73D}

Die Anwendung wird automatisch deinstalliert.

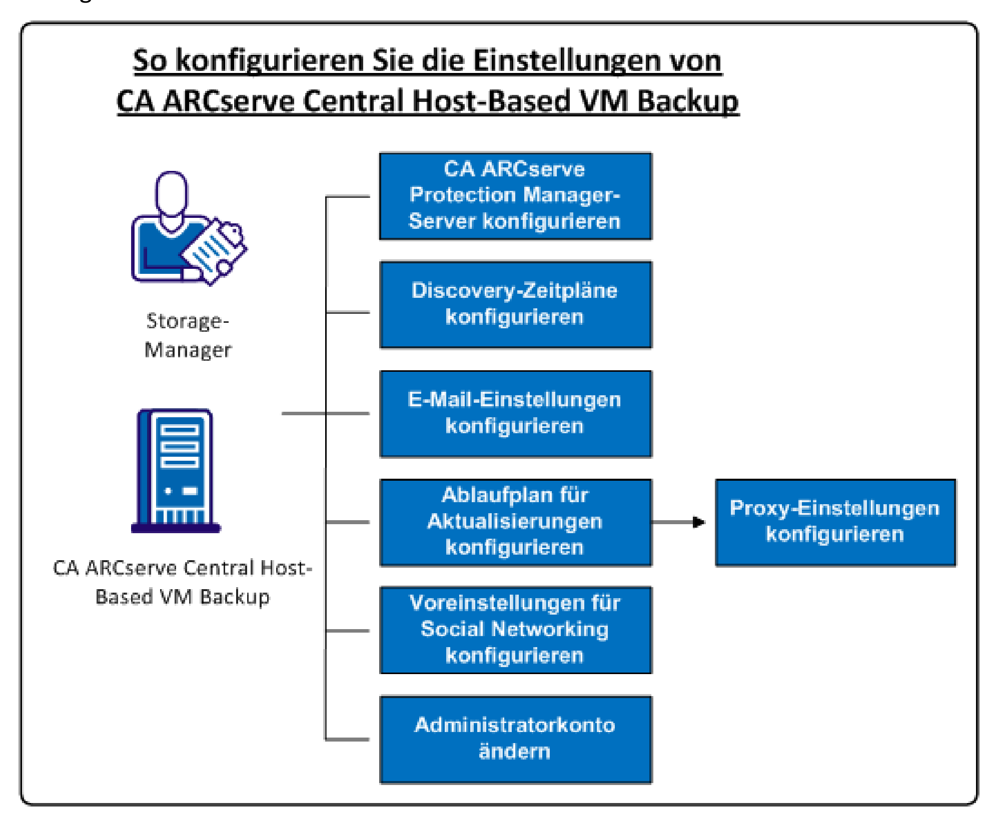
Konfigurieren von CA ARCserve Central Host-Based VM Backup, um CA ARCserve D2D-Knoten zu schützen

Die Anwendung lässt Sie Konfigurationseinstellungen für E-Mail-Warnungen und Ablaufpläne angeben, und Sie können entscheiden, wie Ihre CA ARCserve Central Host-Based VM Backup-Installation aktualisiert werden soll.

Bevor Sie anfangen, Ihre Konfigurationseinstellungen anzugeben, müssen Sie CA ARCserve D2D auf dem Server installieren, der Ihre Sicherungsjobs ausführen wird. Bei diesem Peer- bzw. Proxy-Server kann es sich je nach Ihren Anforderungen um einen einzelnen oder mehrere Rechner handeln. Weitere Anweisungen finden Sie im Abschnitt Installieren von CA ARCserve D2D im CA ARCserve D2D-Benutzerhandbuch.

Sie können CA ARCserve Central Host-Based VM Backup auf demselben oder einem separaten Rechner installieren. Der Installationsvorgang ist assistentenbasiert, was das Setup erleichtert. Weitere Informationen finden Sie unter Installieren von CA ARCserve Central Host-Based VM Backup.

Die folgende Abbildung beschreibt die Konfigurationstypen, die Sie für Ihre Anwendung festlegen können:



Dieses Szenario enthält folgende Themen:

- Konfigurieren des CA ARCserve Central Protection Manager-Servers (siehe Seite 29)

Konfigurieren des CA ARCserve Central Protection Manager-Servers

Beim Konfigurieren des CA ARCserve Central Protection Manager-Servers können Sie die aktuellen Einstellungen von CA ARCserve Central Host-Based VM Backup in CA ARCserve Central Protection Manager-Server-Einstellungen ändern. Wenn die Einstellungen konfiguriert werden, können Sie in CA ARCserve Central Reporting die E-Mail-Alert-Informationen für die erkannten Knoten von Host-Based VM Backup anzeigen.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim CA ARCserve Central Host-Based VM Backup-Server an, und klicken Sie in der Navigationsleiste auf "Konfiguration".

   Der Bildschirm "Konfiguration" wird angezeigt.

2. Klicken Sie im Konfigurationsbereich auf "CA ARCserve Central Protection Manager-Konfiguration".

3. Füllen Sie die folgenden Felder aus:

   - **CA ARCserve Central Protection Manager-Server**

     Hinweis: Wenn CA ARCserve Central Protection Manager und CA ARCserve Central Host-Based VM Backup installiert sind, zeigen die folgenden Felder standardmäßig den lokalen CA ARCserve Central Protection Manager-Server an. Wenn CA ARCserve Central Protection Manager nicht installiert ist, bleiben die Felder leer und Sie müssen die Konfiguration manuell vornehmen. Sie können die Warnungsinformationen zu erkannten Knoten von CA ARCserve Central Reporting anzeigen.

- **Rechnername**: Der Hostname des Computers, auf dem CA ARCserve Central Protection Manager installiert ist.
- **Benutzername:** Der Benutzername, der erforderlich ist, um sich beim Computer anzumelden, auf dem CA ARCserve Central Protection Manager installiert ist.
- **Kennwort:** Das Kennwort des Benutzers.
- **Port:** Die Portnummer an, die Sie verwenden müssen, um mit dem CA ARCserve Central Protection Manager-Webdienst zu kommunizieren.
- **HTTPS:** Diese Option ist je nach der Verbindungskonfiguration auf dem CA ARCserve Central Protection Manager-Server aktiviert oder deaktiviert.

- **Port und Protokoll automatisch erkennen**: Ermöglicht es Ihnen, CA ARCserve Central Protection Manager-Port und -Protokoll der Datenbank des Protection Manager abzurufen, und füllt die oben aufgeführten Felder auf.

  Hinweis: Diese Option ist nur aktiviert, wenn der Remote-Zugriff für die Registrierung des CA ARCserve Central Protection Manager-Servers erlaubt ist.

  Um zu überprüfen, ob der Remote-Zugriff auf die Registrierung erlaubt ist oder nicht, führen Sie die folgenden Schritte aus:

  1. Navigieren Sie zu dem CA ARCserve Central Protection Manager-Server, auf dem CA ARCserve Central Protection Manager installiert ist.

  2. Navigieren Sie zu "services.msc" und stellen Sie sicher, dass der Remote-Registrierungsdienst gestartet ist.

  3. Stellen Sie auf "Automatisch" ein.

- **Test**: Ermöglicht es Ihnen, zu überprüfen, ob die Zugriffsinformationen für CA ARCserve Central Protection Manager korrekt sind.

4. Klicken Sie auf "Speichern".

Konfigurieren von Discovery-Ablaufplänen

Für den Discovery-Ablaufplan für Knoten können Sie einen bestimmten Zeitpunkt und das Wiederholungsintervall konfigurieren. Standardmäßig ist "Discovery-Konfiguration" deaktiviert. Um die Konfiguration zu aktivieren, klicken Sie auf die Option "Aktivieren", um die von Ihnen gewünschte Wiederholungsmethode und einen bestimmten Zeitpunkt für den Beginn der Knoten-Discovery festzulegen. Sie können die folgenden Parameter festlegen, um Ihren Discovery-Ablaufplan zu konfigurieren:

- **Nach folgender Anzahl von Tagen:** Lässt Sie die Methode nach der angegebenen Anzahl von Tagen wiederholen. (Standard)
- **Alle ausgewählten Tage der Woche:** Lässt Sie die Methode an den angegebenen Tagen wiederholen. Montag, Dienstag, Mittwoch, Donnerstag und Freitag sind die standardmäßigen Wochentage.
- **Alle ausgewählten Tage des Monats:** Lässt Sie die Methode am angegebenen Tag des Monats wiederholen. 1 ist die Standardoption für den Tag des Monats.

Eine vCenter/ESX-Host-Liste wird angezeigt, wenn Sie einen Ablaufplan zur Knotenerkennung einrichten.

Konfigurieren von E-Mail- und Alert-Einstellungen

Sie können die E-Mail- und Alert-Einstellungen für die Verwendung mit Ihrer Anwendung konfigurieren, um gemäß der Bedingungen, die Sie angeben, automatische Warnmeldungen zu versenden.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste der Startseite auf "Konfiguration" um die Ansicht "Konfiguration" zu öffnen.

2. Klicken Sie vom Konfigurationsbereich auf "E-Mail- und Alert-Konfiguration", um die E-Mail- und Alert-Konfigurationsoptionen zu öffnen.

3. Füllen Sie die folgenden Felder aus:
   - **Dienst**: Geben Sie im Drop-down-Feld den Typ des E-Mail-Dienstes. (Google Mail, Yahoo Mail, Live Mail oder andere)
   - **E-Mail-Server**: Geben Sie den Hostnamen des SMTP-Servers an, den CA ARCserve Central Applications verwenden soll, um E-Mails zu senden.
   - **Erfordert Authentifizierung**: Wählen Sie diese Option aus, wenn der angegebene E-Mail-Server, Authentifizierung benötigt. Der Kontoname und das Kennwort müssen angegeben werden.
   - **Betreff**: Geben Sie einen standardmäßigen E-Mail-Betreff an.
   - **Von**: Geben Sie die E-Mail-Adresse an, von der die E-Mail geschickt wird.
   - **Empfänger**: Geben Sie eine oder mehrere durch Semikolon (;) getrennte E-Mail-Adressen an, an die die E-Mail geschickt wird.
   - **SSL verwenden**: Wählen Sie diese Option aus, wenn der angegebene E-Mail-Server eine sichere Verbindung (SSL) erfordert.
   - **STARTTLS senden**: Wählen Sie diese Option aus, wenn der angegebene E-Mail-Server einen STARTTLS-Befehl erfordert.
   - **HTML-Format verwenden**: Ermöglicht es Ihnen, die E-Mails in HTML-Format zu senden. (Standardmäßig ausgewählt)
   - **Proxy-Einstellungen aktivieren**: Wählen Sie diese Option aus, wenn ein Proxy-Server vorhanden ist, und geben Sie anschließend die Proxy-Server-Einstellungen an.
4. Klicken Sie auf "Test-E-Mail", um zu sicherzustellen, dass die E-Mail-Konfigurationseinstellungen richtig sind.
5. (Optional) Klicken Sie im Bereich "E-Mail-Alerts senden" auf "Erkannte Knoten", um die Anwendung E-Mail-Warnungs-Meldungen senden zu lassen, wenn neue Knoten entdeckt werden.
6. Klicken Sie auf "Speichern".

   Hinweis: Sie können auf "Zurücksetzen" klicken, um zu den früher gespeicherten Werten zurückzukehren, oder auf "Löschen", um Ihre gespeicherten Einstellungen zu löschen. Das Löschen Ihrer E-Mail- und Alert-Einstellungen hat zur Folge, dass Sie keine E-Mail-Warnungs-Meldungen empfangen.

Die E-Mail-Konfiguration wird angewendet.

Konfigurieren von Ablaufplänen für Aktualisierungen

Mit der Anwendung können Sie einen Ablaufplan einrichten, der automatisch Produktaktualisierungen von einem CA-Server oder einem lokalen Software-Staging-Server herunterlädt.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.
2. Klicken Sie in der Navigationsleiste auf "Konfiguration", um die Ansicht "Konfiguration" zu öffnen.
3. Klicken Sie im Konfigurationsbereich auf "Konfiguration aktualisieren".

   Die Optionen für die Aktualisierung der Konfiguration werden angezeigt.
4. Wählen Sie einen Download-Server aus.
   - **CA-Server:** Klicken Sie für folgende Optionen auf "Proxy-Einstellungen":
     - **Proxy-Einstellungen des Browsers verwenden:** Lässt Sie die Anmeldeinformationen verwenden, die für die Proxy-Einstellungen des Browsers vorbereitet wurden.

       Hinweis: Die Option "Proxy-Einstellungen des Browsers verwenden" wirkt sich auf Internet Explorer und Chrome aus.
     - **Proxy-Einstellungen konfigurieren:** Legen Sie die IP-Adresse oder den Hostnamen des Proxy-Servers und die Portnummer fest. Wenn der Server, den Sie angegeben haben, Authentifizierung erfordert, klicken Sie auf die Option "Proxy-Server erfordert Authentifizierung" und geben Sie die Anmeldeinformationen ein.

       Klicken Sie auf "OK", um zur Konfiguration der Aktualisierung zurückzukehren.
   - **Staging-Server**: Wenn Sie diese Option auswählen, klicken Sie auf "Server hinzufügen", um einen Staging-Server zur Liste hinzuzufügen. Geben Sie seinen Hostnamen und die Portnummer ein, und klicken Sie auf "OK".

     Wenn Sie mehrere Staging-Server angeben, versucht die Anwendung, den ersten der aufgelisteten Server zu verwenden. Wenn die Verbindung erfolgreich ist, werden die verbleibenden aufgelisteten Server nicht für das Staging verwendet.
5. (Optional) Klicken Sie auf "Verbindung testen", um die Serververbindung zu überprüfen und warten Sie, bis der Test abgeschlossen ist.
6. (Optional) Klicken Sie auf die Option "Automatisch nach Aktualisierungen suchen" und legen Sie den Tag und die Zeit fest. Sie können einen täglichen oder wöchentlichen Ablaufplan angeben.

Klicken Sie auf "Speichern", um die Konfiguration der Aktualisierung anzuwenden.

Proxy-Einstellungen konfigurieren

CA ARCserve Central Applications lässt Sie einen Proxy-Server zur Kommunikation mit CA Support festlegen, um nach verfügbaren Aktualisierungen zu überprüfen und sie herunterzuladen. Um diese Möglichkeit zu aktivieren, geben Sie den Proxy-Server an, mit dem Sie anstelle des CA ARCserve Central Applications-Servers kommunizieren wollen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Konfiguration".

   Die Konfigurationsoptionen werden angezeigt.

2. Klicken Sie auf "Konfiguration aktualisieren".

   Die Optionen für die Aktualisierung der Konfiguration werden angezeigt.

3. Klicken Sie auf Proxy-Einstellungen.

   Das Dialogfeld "Proxy-Einstellungen" wird geöffnet.

4. Aktivieren Sie eine der folgenden Optionen:

   - **Proxy-Einstellungen des Browsers verwenden:** Lässt die Anwendung die gleichen Proxy-Einstellungen erkennen und verwenden, die auf den Browser angewendet werden, um für den Erhalt von Aktualisierungsinformationen mit dem CA Technologies-Server zu kommunizieren.

     Hinweis: Dieses Verhalten bezieht sich nur auf Internet Explorer- und Chrome-Browser.

   - **Proxy-Einstellungen konfigurieren:** Lässt Sie einen alternativen Server festlegen, den die Anwendung verwenden wird, um mit CA Support zu kommunizieren und nach Aktualisierungen zu prüfen. Der alternative Server (Proxy) hilft dabei, mehr Sicherheit, erhöhte Leistung und Verwaltungskontrolle zu bieten.

     Füllen Sie die folgenden Felder aus:

     - **Proxy-Server:** Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers an.

     - **Port:** Geben Sie die Portnummer an, die der Proxy-Server verwenden wird, um mit der CA Support-Website zu kommunizieren.

     - **(Optional) Proxy-Server erfordert Authentifizierung:** Falls die Anmeldeinformationen für den Proxy-Server nicht die gleichen sind wie die Anmeldeinformationen für den CA ARCserve Central Applications-Server, aktivieren Sie das Kontrollkästchen neben "Proxy-Server erfordert Authentifizierung" und legen Sie den Benutzernamen und das Kennwort fest, die erforderlich sind, um sich beim Proxy-Server anzumelden.

       Hinweis: Verwenden Sie das folgende Format, um den Benutzernamen anzugeben: <Domänenname>\<Benutzername>.

   Klicken Sie auf "OK".

Die Proxy-Einstellungen sind konfiguriert.

Hinweis: Um dazu beizutragen, dass CA ARCserve Central Host-Based VM Backup Richtlinien für Knoten bereitstellen und CA ARCserve D2D-Knoten schützen kann, stellen Sie sicher, dass der Host-Based VM Backup-Server und der Proxy-Server über ihre Hostnamen miteinander kommunizieren können. Führen Sie die folgenden Schritte aus:

1. Pingen Sie vom CA ARCserve Central Host-Based VM Backup-Server aus den Proxy-Server an, indem Sie den Hostnamen des Servers verwenden.

2. Pingen Sie vom Proxy-Server aus den CA ARCserve Central Host-Based VM Backup-Server an, indem Sie den Hostnamen des Servers verwenden.

Konfigurieren von Voreinstellungen für Social Networking

CA ARCserve Central Applications lässt Sie die Social Networking-Tools verwalten, die Ihnen dabei helfen, die Anwendung zu verwalten. Sie können Nachrichten-Feeds generieren, Verknüpfungen zu beliebten Social Networking-Websites angeben und Videoquellen-Websites auswählen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste der Startseite auf "Konfiguration" um die Ansicht "Konfiguration" zu öffnen.

2. Klicken Sie im Konfigurationsbereich auf "Konfiguration der Voreinstellungen", um die Voreinstellungsoptionen zu öffnen.



3. Legen Sie die benötigten Optionen fest.

   - **Nachrichten-Feed:** Ermöglicht es, dass die Anwendung RSS-Feeds über mit CA ARCserve Central Applications und CA ARCserve D2D in Zusammenhang stehenden Nachrichten und Produktinformationen (aus dem Expertenforum) anzeigt. Die Feeds werden auf der Startseite angezeigt.
   - **Social Networking:** Ermöglicht es, dass die Anwendung auf der Startseite Zugriffssymbole auf Twitter und Facebook für mit CA ARCserve Central Applications und CA ARCserve D2D im Zusammenhang stehende Social Networking-Websites anzeigt.
   - **Videos:** Ermöglicht es Ihnen, den Videotyp auszuwählen, um Ihre Produkte von CA ARCserve Central Applications und CA ARCserve D2D anzuzeigen. ("YouTube-Videos verwenden" ist das Standardvideo.)

   Klicken Sie auf "Speichern".

   Die Social Networking-Optionen werden angewendet.

4. Klicken Sie in der Navigationsleiste auf "Start".

   Die Startseite wird geöffnet.

5. Aktualisieren Sie Ihren Browser.

   Die Social Networking-Optionen werden angewendet.

Ändern des Administratorkontos

CA ARCserve Central Applications lässt Sie den Benutzernamen, das Kennwort, oder beides für das Administratorkonto ändern, nachdem Sie die Anwendung installiert haben. Dieses Administratorkonto wird im Anmeldefenster nur für den standardmäßigen Anzeigebenutzernamen verwendet.

Hinweis: Der angegebene Benutzername muss ein Windows-Administratorkonto oder ein Konto sein, das Windows-Administratorrechte hat.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Konfiguration".

   Die Konfigurationsoptionen werden angezeigt.

2. Klicken Sie auf "Administratorkonto".

3. Die Administratorkontoeinstellungen werden angezeigt.

4. Aktualisieren Sie folgende Felder je nach Bedarf:

   - Benutzername
   - Kennwort

   Klicken Sie auf "Speichern".

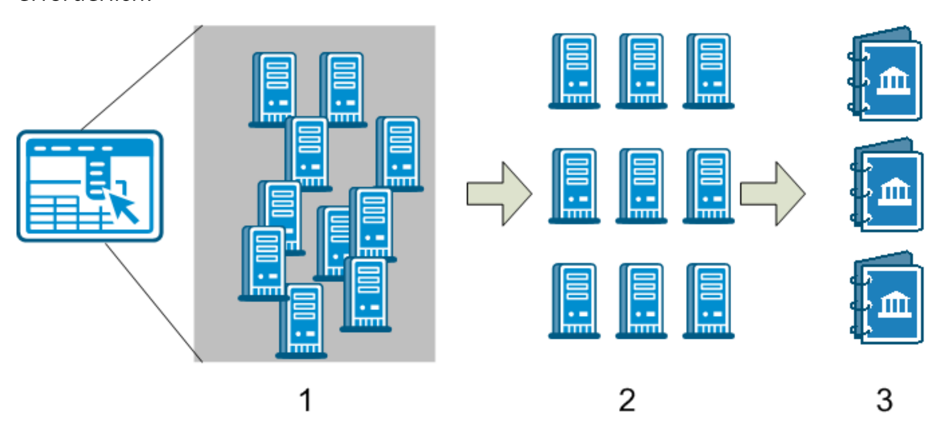
Das Administratorkonto wurde geändert.

Kapitel 3: Mithilfe von CA ARCserve Central Host-Based VM Backup:

Dieses Kapitel enthält folgende Themen:

So richten Sie Ihre Produktionsumgebung ein

Für den Schutz Ihre virtuellen Rechnerumgebung sind einige grundlegende Schritte erforderlich:



1. Fügen Sie die Knoten zu CA ARCserve Central Host-Based VM Backup hinzu. Sie können alle von einem ESX- oder vCenter-Server gehosteten virtuellen Rechner importieren.
2. Teilen Sie die Knoten in Gruppen ein, um ihre Verwaltung einfacher zu gestalten. Sie können Knoten beispielsweise nach Geschäftsfunktion oder nach installierten Anwendungen gruppieren.
3. Erstellen Sie Sicherungsrichtlinien und weisen Sie einer Richtlinie einen Knoten zu. Alle Knoten werden entsprechend der von Ihnen festgelegten Richtlinie gesichert.

So verwenden Sie die CA ARCserve Central Host-Based VM Backup-Startseite

Wenn Sie CA ARCserve Central Host-Based VM Backup starten, wird die Startseite in Ihrem Web-Browser geöffnet. Auf der Startseite können Sie folgende Aufgaben durchführen:

- **Linker Navigationsbereich**:
  - **Knoten**: Auf der Ansicht "Knoten" können Sie Ihre virtuelle Rechnerumgebung nach Knotengruppen, installierten Anwendungen und zugewiesener vSphere-Richtlinie anzeigen.
  - **Richtlinien**: Auf der Ansicht "vSphere-Richtlinien" können Sie Sicherungsrichtlinien für alle Knoten in Ihrer Umgebung erstellen, bearbeiten und zuweisen.
  - **Konfiguration**: Auf der Ansicht "Konfiguration" können Sie E-Mail-Warmmeldungen und Ablaufpläne für automatische Aktualisierungen für die Anwendung einrichten.
  - **Protokolle anzeigen**: Auf der Ansicht "Protokolle anzeigen" finden Sie folgende Themen: Informationen, Fehler oder Warnungen.
  - **Neue Registerkarte hinzufügen**: Sie können die Namen und URLs der Websites, die Sie überwachen möchten, manuell hinzufügen.
  - **CA Support**: Ermöglicht Ihnen den Zugriff auf verschiedene Support- und Social Network-Seiten einschließlich Facebook und Twitter.

Anmelden bei CA ARCserve D2D-Knoten

Auf der Host-Based VM Backup-Startseite können Sie sich bei CA ARCserve D2D-Knoten anmelden.

So melden Sie sich bei CA ARCserve D2D-Knoten an

1. Öffnen Sie die Anwendung und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

3. Suchen und klicken Sie auf den Knoten, auf dem Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

   Eine CA ARCserve Central Host-Based VM Backup-Version von CA ARCserve D2D wird geöffnet.

   Hinweis: Wenn sich ein neues Browser-Fenster nicht öffnet, stellen Sie sicher, dass die Pop-up-Optionen für Ihren Browser alle Pop-up-Fenster oder Pop-up-Fenster nur auf dieser Website zulassen.

Sie sind beim CA ARCserve D2D-Knoten angemeldet.

Hinweis: Wenn Sie sich das erste Mal beim CA ARCserve D2D-Knoten anmelden, wird möglicherweise eine HTML-Seite geöffnet, die eine Warnmeldung anzeigt. Dies kann bei Verwendung von Internet Explorer auftreten. Um dieses Problem zu lösen, schließen Sie Internet Explorer und wiederholen Sie die Schritt 3. Danach sollten Sie sich problemlos beim CA ARCserve D2D-Knoten anmelden können.

So verwalten Sie Knotenaufgaben für CA ARCserve Central Host-Based VM Backup

Dieses Szenario erklärt, wie Speicheradministratoren Knoten verwalten können. Zum Beispiel wird das Hinzufügen oder Erkennen, das Zuweisen von Knoten zu Knotengruppen, und das Aktualisieren oder Löschen von Knoten aus der Ansicht "Knoten löschen" beschrieben.

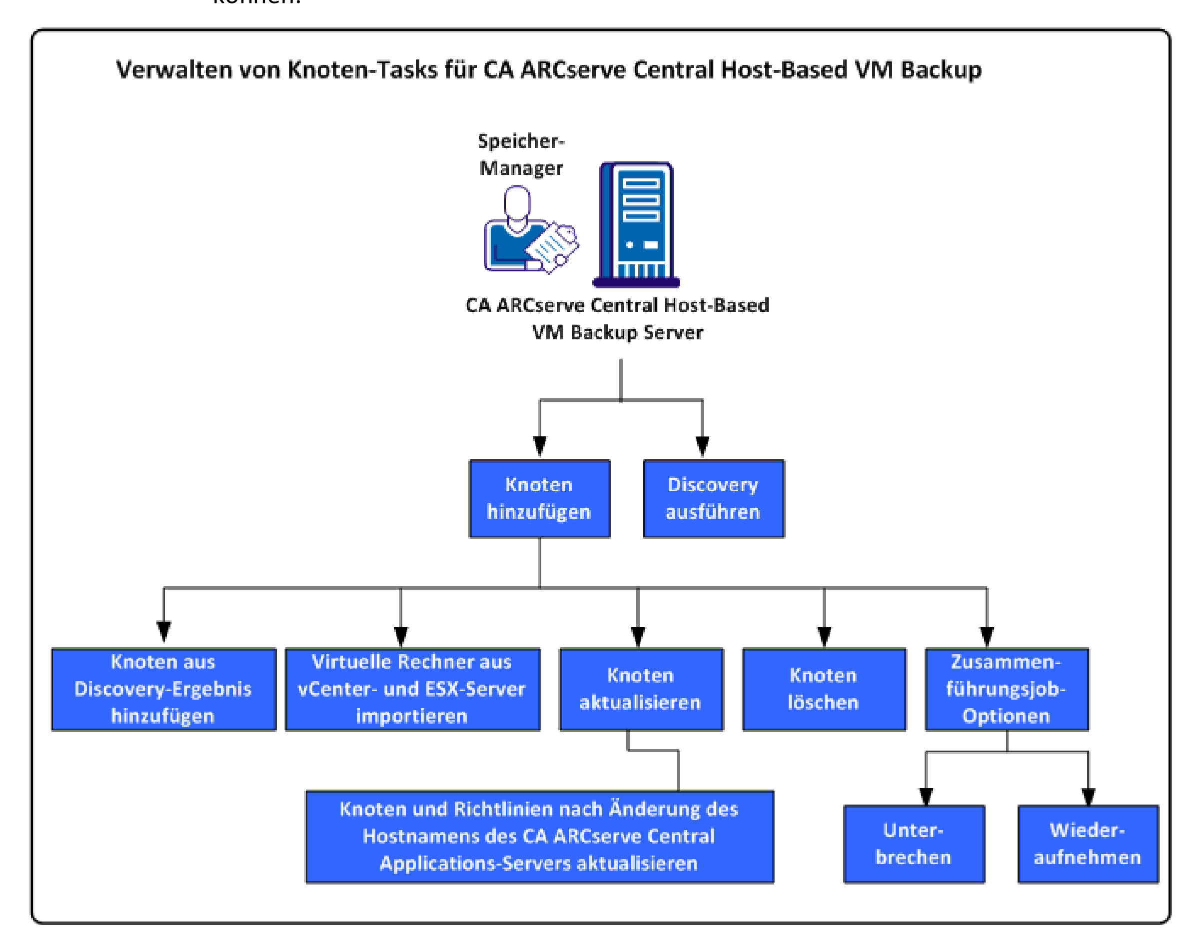
Die folgende Tabelle beschreibt die Elemente, die auf der Ansicht "Knoten" angezeigt werden:

Spaltenname	Beschreibung
Knotenname	Zeigt den Namen des Knotens an. **Hinweis**: Einige der aufgelisteten Knoten stehen Ihnen möglicherweise nicht zur Auswahl zur Verfügung. Das liegt daran, dass der Knoten vom Server nicht erkannt werden kann. Zum Beispiel kann der Knoten aus dem Server gelöscht werden.
Richtlinie	Zeigt den Namen der Richtlinie und den Richtlinienbereitstellungsstatus an.
Name des virtuellen Rechners	Zeigt den Namen des virtuellen Rechners an.
vCenter/ESX	Zeigt die Serverdetails an, die dabei helfen, virtuelle Rechner zu erkennen.
Job (siehe Seite 75)	Zeigt den Status des Sicherungsjobs an und leitet Sie weiter an die Statusüberwachung der Sicherung (siehe Seite 76) für weitere Details.

Spaltenname	**Beschreibung**
Status	Zeigt den Namen des Knotenstatus an. ■ = Fehler/Fehlgeschlagen ■ = Warnung ■ = Erfolgreich Wenn Sie Ihren Mauszeiger über das Symbol bewegen, wird die Pop-up-Tabelle "Knotenstatusübersicht" mit Ergebnissen für die folgenden Kategorien angezeigt: ■ Letzte Sicherung: Zeigt den Typ, das Datum, die Uhrzeit und den Status der Sicherung an. ■ Wiederherstellungspunkte: Zeigt die Anzahl der Wiederherstellungspunkte für den überwachten Server. ■ Zielkapazität: Zeigt den freien Speicherplatz Ihres Sicherungsziels an.
Ergebnis der letzten Sicherung	Zeigt den Status des letzten Sicherungsjobs an.
Zuletzt gesichert um	Zeigt das Datum und die Uhrzeit des letzten Sicherungsjobs an.
PFC-Status	Zeigt den Status des Preflight-Checks für Ihre Sicherungsjobs an: ■ = Fehler/Fehlgeschlagen ■ = Warnung ■ = Erfolgreich Das Symbol bestimmt, ob für den jeweiligen Knoten ein Sicherungsjob ausgeführt werden kann oder nicht. Wenn Sie Ihren Mauszeiger über das Symbol bewegen, wird die Pop-up-Tabelle "Überprüfung" mit Ergebnissen für die folgenden Kategorien angezeigt: ■ Verfolgung geänderter Blöcke (CBT): Zeigt das Ergebnis der Verfolgung geänderter Blöcke für die Sicherung an. ■ VMware-Tools: Zeigt an, ob das VMware-Tool installiert ist oder nicht. ■ Datenträger: Zeigt den Status des Datenträgers an. ■ Power-Status: Zeigt an, ob der virtuelle Rechner ein- oder ausgeschaltet ist. ■ Anmeldeinformationen: Zeigt den Status der Benutzeranmeldeinformationen an. ■ Anwendungen: Zeigt den Installationsstatus der Anwendung auf dem Knoten an. Weitere Details finden Sie unter dem Thema Preflight-Checks Ihrer Sicherungen ausführen (siehe Seite 62).
Anwendungen	Zeigt die Anwendung an, dem der Knoten zugeordnet ist.

Spaltenname	Beschreibung
BS	Zeigt das Betriebssystem an, dem der Knoten zugeordnet ist.
Beschreibung	Zeigt eine Beschreibung des Knotens an.

Das folgende Diagramm veranschaulicht die Aufgaben, die Sie auf Knoten ausführen können.



Dieses Szenario beschreibt die Optionen, die Sie verwenden können, wenn Knoten hinzugefügt oder aktualisiert werden:

- Erkennen (siehe Seite 46)
- Hinzufügen von Knoten (siehe Seite 47)
  - Automatisches Hinzufügen von Knoten vom Auto Discovery-Ergebnis (siehe Seite 48)
  - Importieren virtueller Rechner aus vCenter- und ESX-Servern (siehe Seite 49)
- Aktualisieren von Knoten (siehe Seite 51)
  - Aktualisieren von Knoten und Richtlinien nach einer Änderung des Hostnamens des CA ARCserve Central Applications-Servers (siehe Seite 52)
- Löschen von Knoten (siehe Seite 52)
- Zusammenführungsjob-Optionen (siehe Seite 53)
  - Zusammenführungsjob auf einem Knoten unterbrechen (siehe Seite 53)

– Zusammenführungsjob auf einem Knoten wiederaufnehmen (siehe Seite 54)

Erkennen von Knoten aus CA ARCserve Central Host-Based VM Backup

CA ARCserve Central Host-Based VM Backup lässt Sie Knoten durch das Hinzufügen von vCenter-Server und ESX-Server-Systemen zu Ihrer Umgebung automatisch erkennen. Durch das Hinzufügen kann die Anwendung automatisch virtuelle Rechner erkennen, die sie hosten.

Wichtig! Der Knotenerkennungsprozess erfordert, dass Sie den Hostnamen oder die IP-Adresse von vCenter- Server oder ESX Server-System angeben. Dank dieser Information erkennt der Discovery-Prozess virtuelle Rechner, die mit dem vCenter-Server und den ESX Server-Systemen verbunden sind. Falls Sie es für notwendig erachten, den Hostnamen oder die IP-Adresse eines vCenter-Servers oder eines ESX Server-Systems zu ändern, wiederholen Sie die in diesem Abschnitt dargestellten Schritte und stellen Sie die Sicherungsrichtlinie erneut bereit, um einen neuen Sicherungssatz mit aktualisiertem Hostnamen bzw. aktualisierter IP-Adresse zu erstellen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.
2. Klicken Sie in der Symbolleiste auf "Erkennen", um das Dialogfeld "Knoten durch vCenter-/ESX-Server erkennen" zu öffnen.
3. Vervollständigen Sie folgende Felder im Dialogfeld "Knoten durch vCenter-/ESX-Server erkennen":
   - vCenter/ESX-Host
   - Benutzername

     Hinweis: Das von Ihnen angegebene Konto muss ein Konto mit Administratorrechten auf dem ESX-Server- oder vCenter-Server-System sein.
   - Kennwort
   - Port

   Klicken Sie auf "Hinzufügen".

   Hinweis: Wiederholen Sie diesen Schritt, um weitere Center/ESX-Server-Systeme hinzuzufügen.
4. Klicken Sie auf "Erkennen", um den Discovery-Vorgang zu starten.

   Der Discovery-Überwachungsserver wird geöffnet und zeigt den Discovery-Fortschritt an.

5. Wenn der Discovery-Fortschritt fertig gestellt ist, wird eine Bestätigungsmeldung angezeigt: Möchten Sie weitere Knoten aus dem Discovery-Ergebnis hinzufügen?

   Klicken Sie auf "Ja" und die Ansicht "Knoten aus Discovery-Ergebnis hinzufügen" wird angezeigt. Klicken Sie auf "Nein", wenn Sie weitere Hypervisoren hinzufügen möchten.

   Hinweis: Wie Sie Knoten automatisch erkennen und sie zur Liste der Knotennamen hinzufügen finden Sie detailliert beschrieben unter dem Thema "Konfigurieren von Discovery-Ablaufplänen".

6. Klicken Sie in der Liste "Erkannte Knoten" auf die Knoten, die Sie hinzufügen möchten, und klicken Sie anschließend auf den rechten Pfeil. Die Knoten werden der Liste "Zu schützende Knoten" hinzugefügt.

7. Klicken Sie auf "Weiter", um das Fenster "Knoten-Anmeldeinformationen" zu öffnen.

8. Geben Sie einen Benutzernamen und Kennwort für jeden Knoten an, den Sie hinzufügen möchten, oder geben Sie die entsprechenden globalen Anmeldeinformationen an.

   Klicken Sie auf Fertig stellen.

   Die von Ihnen ausgewählten Knoten werden im Fenster "Knoten" der Liste "Knotennamen" für die ausgewählte Knotengruppe hinzugefügt.

9. (Optional) Klicken Sie auf "Aktualisieren". Der von Ihnen hinzugefügte Server wird nun im Fenster "Knoten" in der Liste "Gruppen" aufgelistet.

10. (Optional) Klicken Sie auf "Erkennen" und wiederholen Sie die vorherigen Schritte, bis alle Server hinzugefügt sind.

Hinzufügen von Knoten

Um auf das Wachstum Ihrer Umgebung zu reagieren, können Sie das Fenster "Knoten" verwenden, um Knoten hinzuzufügen und diese anschließend zu Gruppen zuzuweisen, die innerhalb der Anwendung verwaltet werden sollen. Die Anwendung fügt nur virtuelle Rechner hinzu auf denen:

- das Gast-BS Windows ist.
- die VMware-Hardwareversion 7 oder höher ist.

Sie können Knoten mithilfe der folgenden Prozesse hinzufügen:

- Knoten aus Discovery-Ergebnis hinzufügen (siehe Seite 48): Discovery ermöglicht es Ihnen, Details für ESX- und vCenter-Server einzugeben, virtuelle Rechner, die auf allen Servern ausgeführt werden, zu erkennen. Die erkannten Knoten können anschließend manuell oder automatisch zur Anwendung hinzugefügt werden, in der sie verwaltet und geschützt werden können.

  Server, die der Discovery-Liste hinzugefügt wurden, werden entsprechend dem im Fenster "Konfiguration" angegebenen Ablaufplan durchsucht, bis Sie sie entfernen. Sie brauchen die Serverdetails nicht erneut eingeben. Die Discovery-Liste zeigt nur neue virtuelle Rechner an, die seit dem letzten Scan einem Server hinzugefügt wurden. Die bereits in der Anwendung verwalteten VMs werden nicht angezeigt. Sie können auch Discovery ausführen, ohne auf den nächsten geplanten Scan zu warten.

- Virtuelle Rechner aus vCenter/ESX importieren (siehe Seite 49)

  Diese Option ist ein manueller Prozess. Der Prozess erfordert, dass Sie bei jedem Starten die Details des ESX- oder vCenter-Servers angeben. Sie können der Discovery-Liste Server hinzufügen, wenn Sie vermeiden möchten, Serverdetails erneut eingeben zu müssen. Diese Option listet alle auf dem angegebenen Server erkannten virtuellen Rechner auf, auch wenn sie bereits in der Anwendung verwaltet werden.

Hinzufügen von Knoten vom Discovery-Ergebnis

Diese Option lässt Sie die Knoten auswählen, die automatisch erkannt werden auf der Basis der Einstellungen, die Sie im Feld "Discovery-Konfiguration" angegeben haben.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Klicken Sie in der Kategorie "Knoten" auf "Hinzufügen" und danach im Pop-up-Menü auf "Knoten aus Discovery-Ergebnis hinzufügen".

   Der Bildschirm "Knoten aus Discovery-Ergebnis hinzufügen" öffnet sich und zeigt eine Liste der erkannten Knoten an.

3. Wählen Sie aus der Liste "Erkannte Knoten" die Knoten aus, die Sie hinzufügen möchten, und klicken Sie auf den Pfeil, um sie zur Liste "Zu schützende Knoten" hinzuzufügen. Klicken Sie zum Abschluss auf "Weiter".

   Hinweis: Sie können die Liste nach Knotennamen oder Domäne filtern, um die Liste zu verkürzen.

4. (Optional) Wählen Sie einen oder mehrere Knoten aus und klicken Sie auf "Ausgewählte Knoten verbergen", um Knoten auszublenden, die Sie nicht sichern wollen.

5. (Optional) Aktivieren Sie die Option "Verborgene Knoten anzeigen", um verborgene Knoten wieder auf der Liste "Erkannte Knoten" anzuzeigen. Um die Knoten wieder auszublenden, deaktivieren Sie die Option.
6. Geben Sie im Fenster "Knoten-Anmeldeinformationen" einen Benutzernamen und ein Kennwort für den Knoten an, den Sie hinzufügen wollen. Sie können globale Anmeldeinformationen angeben oder Anmeldeinformationen auf die ausgewählten Knoten anwenden.
7. Klicken Sie auf Fertig stellen.

Die Knoten werden hinzugefügt.

Virtuelle Rechner aus vCenter/ESX importieren

Sie können Knoten auch mithilfe der Option "Virtuelle Rechner aus ESX/vCenter-Server importieren" hinzufügen. Diese Aufgabe lässt die Anwendung alle virtuellen Rechner erkennen, die auf dem angegebenen Host ausgeführt werden, führt jedoch keine periodischen automatischen Scans aus. Wenn Sie virtuelle Rechner später hinzufügen, müssen Sie diesen Vorgang wiederholen, damit die neuen virtuellen Rechner erkannt werden.

Beachten Sie folgende Unterscheidungen zwischen dieser Option und der Discovery-Option:

- Sie müssen die Details des ESX-Servers und vCenter-Servers jedes Mal festlegen, wenn Sie diese Option starten.
- Sie können jeden angegebenen Server zur Discovery-Liste hinzufügen, sodass Sie die Anmeldeinformationen nicht jedes Mal eingeben müssen.
- Alle verfügbaren virtuellen Rechner werden jedes Mal aufgelistet, wenn Sie diese Option verwenden. Sogar die virtuellen Rechner, die von der Anwendung verwaltet werden, werden aufgelistet.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.
2. Klicken Sie in der Symbolleiste auf "Hinzufügen" und dann im Pop-up-Menü auf "Virtuelle Rechner aus Center/ESX importieren".

   Das Dialogfeld "Knoten erkennen" wird geöffnet.

3. Füllen Sie im Dialogfeld "Knoten erkennen" die folgenden Felder aus:

   - vCenter/ESX-Host

     Hinweis: Geben Sie als eine Best Practice beim Importieren von virtuellen Rechnern den Hostnamen oder die IP-Adresse des vCenter Server-Systems an, wenn Sie in Ihrer Umgebung VMware Distributed Resource Scheduling (DRS) ausführen. Diese Vorgehensweise stellt sicher, dass CA ARCserve Central Host-Based VM Backup die in Ihrer Umgebung ausgeführten virtuellen Rechner erkennen kann und Sicherungen von für DRS aktivierte virtuelle Rechner erfolgreich abgeschlossen werden. Um Sicherungsfehler zu verhindern, wenn virtuelle Rechner zwischen ESX-Servern verschoben werden, wird empfohlen, den Hostnamen bzw. die IP-Adresse des ESX-Servers beim Importieren von virtuellen Rechnern nicht anzugeben.

     Weitere Informationen zu Distributed Resource Scheduler finden Sie auf der VMware-Website.

   - Benutzername
   - Kennwort
   - Port
   - Protokoll

   Klicken Sie auf "Verbinden" und warten Sie, bis das Scannen abgeschlossen ist.

4. (Optional) Aktivieren Sie die Option "vCenter/ESX-Server automatisch zur Discovery-Liste hinzufügen".

5. Klicken Sie auf "Weiter", um das Fenster "Knoten-Anmeldeinformationen" zu öffnen.

6. Geben Sie im Fenster "Knoten-Anmeldeinformationen" einen globalen Benutzernamen und ein Kennwort für alle entdeckten virtuellen Rechner an, und klicken Sie auf die Option "Auf ausgewählte Knoten anwenden". Alternativ können Sie auf eine VM klicken, um bestimmte Anmeldeinformationen einzugeben.

7. Klicken Sie auf Fertig stellen.

Die ausgewählten virtuellen Rechner werden zu der Knotengruppe, die Sie angegeben haben, hinzugefügt.

Hinweis: CA ARCserve Central Host-Based VM Backup kann die Hostnamen von virtuellen Rechnern, die ausgeschaltet sind oder auf denen VMware Tools nicht installiert ist, nicht entdecken. In solchen Fällen wird nach dem Knotenimport im Feld "Hostname" auf dem Fenster "Knoten" "Unbekannt" angezeigt. Zusätzlich kann der Knotennamenfilter (auf dem Fenster "Knoten") keine Knoten mit dem Namen "Unbekannt" filtern.

Aktualisieren von Knoten

CA ARCserve Central Host-Based VM Backup lässt Sie Informationen zu Knoten aktualisieren, die zuvor hinzugefügt wurden.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Wählen Sie in der Navigationsleiste auf der Startseite "Knoten" aus.

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Menüleiste "Gruppen" auf die Gruppe "Alle Knoten" oder klicken Sie auf den Gruppennamen, der die Knoten enthält, die Sie aktualisieren wollen.

   Die der Gruppe zugeordneten Knoten werden in der Knotenliste angezeigt.

3. Klicken Sie auf die Knoten, die Sie aktualisieren möchten, und klicken Sie anschließend mit der rechten Maustaste, und wählen Sie im Pop-up-Menü die Option "Knoten aktualisieren".

   Das Dialogfeld "Knoten aktualisieren" wird geöffnet.

   Hinweis: Um alle Knoten in der Knotengruppe zu aktualisieren, klicken Sie mit der rechten Maustaste auf den Namen "Knotengruppe", und klicken Sie anschließend im Pop-up-Menü auf "Knoten aktualisieren".

4. Aktualisieren Sie die Knotendetails nach Bedarf.

   Hinweis: Um mehrere Knoten mit der rechten Maustaste auf der Knotenliste zu aktualisieren, wählen Sie die gewünschten Knoten aus, klicken Sie mit der rechten Maustaste auf einen Knoten, und klicken Sie dann im Pop-up-Menü auf "Aktualisieren". Benutzername und Kennwort sind für alle ausgewählten Knoten gleich. Standardmäßig sind die Option "Neue Anmeldeinformationen angeben" und das Kontrollkästchen "Steuerung übernehmen für Knoten" aktiviert. Sie können einen neuen Benutzernamen und Kennwort für die ausgewählten Knoten angeben und können diesen Server zwingen, die Knoten zu verwalten. Außerdem können Sie die Option "Vorhandene Anmeldeinformationen verwenden", um den aktuellen Benutzernamen und das aktuelle Kennwort anzuwenden. Die Felder werden deaktiviert.

5. Klicken Sie auf "OK".

   Das Dialogfeld "Knoten aktualisieren" wird geschlossen, und die Knoten werden aktualisiert.

Aktualisieren von Knoten und Richtlinien nach einer Änderung des Hostnamens des CA ARCserve Central Applications-Servers

Nachdem Sie den Hostnamen des CA ARCserve Central Host-Based VM Backup-Servers geändert haben, aktualisieren Sie die Knoten und die Richtlinien, die auf die Knoten angewendet werden. Sie führen diese Aufgaben aus, um die Beziehung zwischen dem Server und den Knoten, die der Server schützt, zu verwalten. In der folgenden Tabelle sind die möglichen Szenarien sowie die entsprechenden Korrekturmaßnahmen beschrieben.

Szenario	Korrekturmaßnahme
Der Knoten wurde hinzugefügt, nachdem der Hostname des CA ARCserve Central Host-Based VM Backup-Servers geändert wurde.	Es sind keine Korrekturmaßnahmen erforderlich.
Der Knoten wurde hinzugefügt, bevor der Hostname des CA ARCserve Central Host-Based VM Backup-Servers geändert wurde, und eine Richtlinie wurde nicht auf den Knoten angewandt.	Aktualisieren Sie den Knoten. Weitere Informationen finden Sie unter Aktualisieren von Knoten (siehe Seite 51).
Der Knoten wurde hinzugefügt, bevor der Hostname des CA ARCserve Central Host-Based VM Backup-Servers geändert wurde, und eine Richtlinie wurde auf den Knoten angewandt.	Wenden Sie die Richtlinie erneut an. Weitere Informationen finden Sie unter Zuweisen von Richtlinien zu virtuellen Rechnern.

Löschen von Knoten

Sie können Knoten nach Bedarf löschen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Klicken Sie in der Menüleiste "Gruppen" auf die Gruppe "Alle Knoten" oder klicken Sie auf den Gruppennamen, der den Knoten enthält, den Sie löschen wollen.

   Die der Gruppe zugeordneten Knoten werden in der Knotenliste angezeigt.

3. Markieren Sie einen oder mehrere Knoten, die Sie löschen wollen, und klicken Sie dann in der Symbolleiste auf "Löschen".

   Eine Bestätigungsmeldung wird angezeigt.

4. Wählen Sie eine der folgenden Vorgehensweisen:

   - Klicken Sie auf "Ja", um den Knoten zu löschen.
   - Klicken Sie auf "Nein", wenn Sie den Knoten nicht löschen wollen.

Zusammenführungsjob-Optionen

CA ARCserve Central Host-Based VM Backup lässt Sie Zusammenführungsjobs für jeden Knoten unterbrechen und jederzeit wiederaufnehmen. Der Prozess des Unterbrechens und Wiederaufnehmens von Zusammenführungsjobs wirkt sich nicht auf Jobs aus, die sich in Bearbeitung befinden.

Zusammenführungsjob auf einem Knoten unterbrechen

CA ARCserve Central Host-Based VM Backup lässt Sie einen Zusammenführungsjob auf einem bestimmten Knoten unterbrechen.

Zum Beispiel können Zusammenführungsjobs Systemressourcen verbrauchen und verursachen, dass Sicherungsjobs verlangsamt ausgeführt werden. Verwenden Sie die Unterbrechungsoption, um einen sich in Bearbeitung befindlichen Zusammenführungsjob anzuhalten, sodass sich in Bearbeitung befindliche Sicherungsjobs mit höchstmöglicher Effizienz abschließen können. Nachdem die Sicherungen abgeschlossen haben, können Sie den Zusammenführungsjob wiederaufnehmen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Startseite von CA ARCserve Central Host-Based VM Backup in der Navigationsleiste auf "Knoten", um das Fenster "Knoten" zu öffnen.
2. Wählen Sie die Knotengruppe aus, die die Knoten mit den Zusammenführungsjobs enthält, die Sie unterbrechen wollen.

   Eine Liste von Knoten für die ausgewählte Knotengruppe wird angezeigt.
3. Klicken Sie auf die Knoten mit den Zusammenführungsjobs, die Sie unterbrechen wollen. Klicken Sie dann mit der rechten Maustaste auf die ausgewählten Knoten und im Pop-up-Menü auf "Zusammenführungsjob unterbrechen".

   Hinweis: Standardmäßig ist die Option "Zusammenführungsjob unterbrechen" deaktiviert. Wenn der Knoten derzeit einen Zusammenführungsjob ausführt, wie in der Job-Spalte angezeigt, wird die Option "Zusammenführungsjob unterbrechen" aktiviert.

Der Zusammenführungsjob des ausgewählten Knotens wird unterbrochen und kann auf der CA ARCserve D2D-Startseite überprüft werden.

Zusammenführungsjob auf einem Knoten wiederaufnehmen

CA ARCserve Central Host-Based VM Backup lässt Sie Zusammenführungsjob wiederaufnehmen, die für einen bestimmten Knoten unterbrochen wurden.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Startseite von CA ARCserve Central Host-Based VM Backup in der Navigationsleiste auf "Knoten", um das Fenster "Knoten" zu öffnen.
2. Wählen Sie die Knotengruppe aus, die die Knoten mit den Zusammenführungsjobs enthält, die Sie wiederaufnehmen wollen.

   Eine Liste von Knoten für die ausgewählte Knotengruppe wird angezeigt.
3. Klicken Sie auf die Knoten mit den Zusammenführungsjobs, die unterbrochen sind, und die Sie nun wiederaufnehmen wollen. Klicken Sie dann mit der rechten Maustaste auf die ausgewählten Knoten und im Pop-up-Menü auf "Zusammenführungsjob wieder aufnehmen".

   Hinweis: Die Option "Zusammenführungsjob wieder aufnehmen" wird aktiviert, wenn kein Sicherungsjob ausgeführt wird und die Zusammenführungsjobs unterbrochen sind.

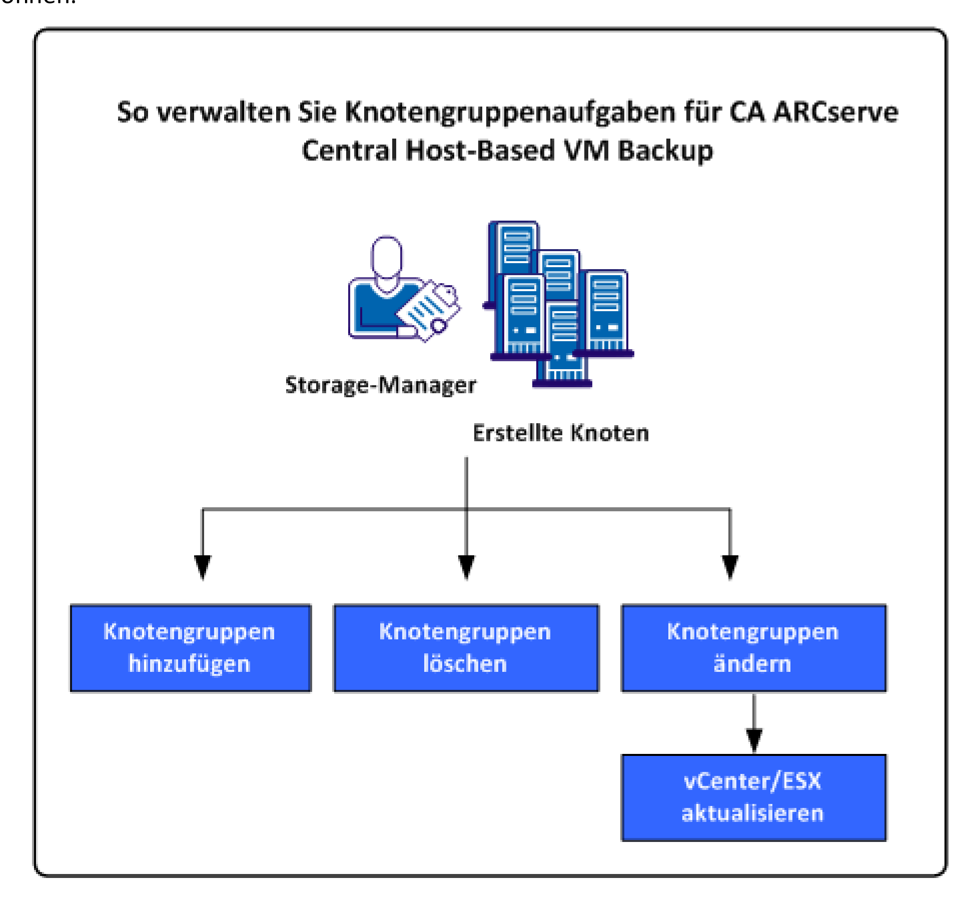
Der Zusammenführungsjob des ausgewählten Knotens wird wieder aufgenommen und kann auf der CA ARCserve D2D-Startseite überprüft werden.

So verwalten Sie Knotengruppenaufgaben für CA ARCserve Central Host-Based VM Backup

Mit CA ARCserve Central Host-Based VM Backup kann ein Speicheradministrator eine Vielzahl an virtuellen Rechnern so einfach schützen, wie einen einzelnen.

Beginnen Sie Knoten hinzuzufügen. Sie können die Knoten nach Anwendung oder nach ihrem Zweck gruppieren. Das Erstellen von Knotengruppen ermöglicht es Ihnen, Ihre virtuelle Rechnerumgebung einfach zu visualisieren. Sie können Sicherungsrichtlinien erstellen und eine Richtlinie zu den Knoten zuweisen, um den Schutz Ihrer virtuellen Umgebung zu vereinfachen. Weitere Details finden Sie unter So verwalten Sie Richtlinien für CA ARCserve Central Host-Based VM Backup (siehe Seite 78).

Die folgende Abbildung beschreibt die Aufgaben, die Sie für Knotengruppen ausführen können:



Dieses Szenario enthält folgende Themen:

- Hinzufügen von Knotengruppen (siehe Seite 56)
- Löschen von Knotengruppen (siehe Seite 58)

- Ändern von Knotengruppen (siehe Seite 59)

Hinzufügen von Knotengruppen

Wenn Sie zuerst einen virtuellen Rechner aus einem ESX- oder vCenter Server-Host importieren, wird eine neue Knotengruppe automatisch hinzugefügt.

Knotengruppen lassen Sie eine Sammlung von auf eine Gemeinsamkeit basierenden CA ARCserve D2D-Quellcomputern verwalten. Zum Beispiel können Sie Knotengruppen definieren, die nach der Abteilung klassifiziert sind, die sie unterstützen: Buchhaltung, Marketing, Recht, Personal, und so weiter.

Die Anwendung enthält die folgenden Knotengruppen:

- **Standardgruppen:**
  - **Alle Knoten--**Enthält alle der Anwendung zugeordneten Knoten.
  - **Knoten ohne Gruppe** -- Enthält alle mit der Anwendung verknüpften Knoten, die keiner Knotengruppe zugewiesen sind.
  - **Knoten ohne Richtlinie** -- Enthält alle mit der Anwendung verknüpften Knoten, denen keine Richtlinie zugewiesen ist.
  - **SQL Server:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft SQL Server ist auf dem Knoten installiert.
  - **Exchange:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft Exchange Server ist auf dem Knoten installiert.

  Hinweis: Sie können die Standardknotengruppen nicht ändern oder löschen.
- **Benutzerdefinierte Gruppen:** Enthält benutzerdefinierte Knotengruppen.
- **vCenter/ESX-Gruppen:** Wenn Sie einen Knoten aus der Option "Virtuelle Rechner aus vCenter/ESX importieren" hinzufügen, wird der Name des vCenter/ESX-Servers zu dieser Gruppe hinzugefügt.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste der Startseite auf "Knoten", um die Ansicht "Knoten" zu öffnen.
2. Klicken Sie in der Symbolleiste "Knotengruppe" auf "Hinzufügen".

   Das Dialogfeld "Gruppe hinzufügen" öffnet sich und die Knoten werden in der Liste der verfügbaren Knoten angezeigt.
3. Geben Sie einen Gruppennamen für die Knotengruppe an.

4. Geben Sie im Dialogfeld "Gruppe hinzufügen" folgende Felder an:

   - **Gruppe:** Wählen Sie den Gruppennamen aus, der die Knoten enthält, die Sie zuweisen möchten.
   - **Knotennamenfilter:** Lässt Sie die verfügbaren Knoten basierend auf einer Gemeinsamkeit filtern.

     Hinweis: Das Feld "Knotenname" unterstützt die Verwendung von Platzhalterzeichen.

     Acc* lässt Sie beispielsweise alle Knoten filtern, die einen Knotennamen haben, der mit "Acc." beginnt. Um die Filterergebnisse zu löschen, klicken Sie im Feld "Filter" auf X.

5. Um Knoten zur Knotengruppe hinzuzufügen, wählen Sie die Knoten aus, die Sie hinzufügen möchten, und klicken Sie auf den einzelnen Rechtspfeil.

   Die Knoten verschieben sich von der Liste "Verfügbare Knoten" zur Liste "Ausgewählte Knoten" und werden der Knotengruppe zugewiesen.

   Hinweis: Um alle Knoten auszuwählen und aus der aktuellen Gruppe zu verschieben, klicken Sie auf den doppelten Rechtspfeil.

6. (Optional) Um Knoten von der Liste "Ausgewählte Knoten" in die Liste "Verfügbare Knoten" zu verschieben, klicken Sie auf den einzelnen Linkspfeil.

   Hinweis: Um alle Knoten auszuwählen und in der aktuellen Gruppe zu verschieben, klicken Sie auf den doppelten Linkspfeil.

7. Klicken Sie auf "OK".

Die Knotengruppe wird hinzugefügt.

Löschen von Knotengruppen

Sie können eine Knotengruppe nach Bedarf löschen. Wenn Sie eine manuell hinzugefügte Gruppe löschen, werden die virtuellen Rechner nicht aus der Anwendung entfernt. Wenn Sie allerdings eine Gruppe löschen, die mit einer ESX- oder vCenter Server-Discovery automatisch erstellt wurde, werden die Gruppe und alle virtuellen Rechner aus der Anwendung gelöscht.

Die Anwendung lässt Sie die Knotengruppen löschen, die Sie erstellt haben.

Sie können folgende Knotengruppen nicht löschen:

- **Alle Knoten--**Enthält alle der Anwendung zugeordneten Knoten.
- **Knoten ohne Gruppe** -- Enthält alle mit der Anwendung verknüpften Knoten, die keiner Knotengruppe zugewiesen sind.
- **Knoten ohne Richtlinie** -- Enthält alle mit der Anwendung verknüpften Knoten, denen keine Richtlinie zugewiesen ist.
- **SQL Server:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft SQL Server ist auf dem Knoten installiert.
- **Exchange:** Enthält alle der Anwendung zugeordneten Knoten, und Microsoft Exchange Server ist auf dem Knoten installiert.

Hinweis: Das Löschen von Knotengruppen löscht keine individuelle Knoten aus der Anwendung.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste der Startseite auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Klicken Sie auf die Knotengruppe, die Sie löschen wollen, und dann in der Symbolleiste der Knotengruppe auf "Löschen".

   Das Meldungsdialogfeld "Bestätigen" öffnet sich.

3. Wenn Sie sicher sind, dass Sie die Knotengruppe löschen möchten, klicken Sie auf "Ja".

   Hinweis: Klicken Sie auf "Nein", wenn Sie die Knotengruppe nicht löschen wollen.

Die Knotengruppe wird gelöscht.

Ändern von Knotengruppen

Die Anwendung lässt Sie die Knotengruppen ändern, die Sie erstellt haben. Sie können Knoten zu Knotengruppen hinzufügen und aus ihnen entfernen und den Namen von Knotengruppen ändern.

Hinweis: Sie können folgende Knotengruppen nicht ändern:

- **Alle Knoten--**Enthält alle der Anwendung zugeordneten Knoten.
- **Knoten ohne Gruppe** -- Enthält alle mit der Anwendung verknüpften Knoten, die keiner Knotengruppe zugewiesen sind.
- **Knoten ohne Richtlinie** -- Enthält alle mit der Anwendung verknüpften Knoten, denen keine Richtlinie zugewiesen ist.
- **SQL Server:** Enthält alle der Anwendung zugeordneten Knoten und Microsoft SQL Server ist installiert.
- **Exchange:** Enthält alle der Anwendung zugeordneten Knoten und Microsoft SQL Server ist installiert.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf der Startseite auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie auf die Knotengruppe, die Sie ändern wollen, und dann in der Symbolleiste der Knotengruppe auf "Ändern".

   Das Dialogfeld "Gruppe ändern" wird geöffnet.

3. Um den Gruppennamen zu ändern, geben Sie einen neuen Namen im Feld "Gruppennamen" an.

4. Um Knoten zur Knotengruppe hinzuzufügen, wählen Sie die Knoten aus, die Sie zur Knotengruppe hinzufügen möchten, und klicken Sie auf den Rechtspfeil.

   Die Knoten verschieben sich von der Liste "Verfügbare Knoten" zur Liste "Ausgewählte Knoten" und werden der Knotengruppe zugewiesen.

   Hinweis: Um alle Knoten von der Liste "Verfügbare Knoten" zur Liste "Ausgewählte Knoten" zu verschieben, klicken Sie auf den doppelten Rechtspfeil.

5. Um Knoten aus der Knotengruppe zu entfernen, klicken Sie auf den linken Pfeil, um einen, oder auf den doppelten Linkspfeil, um alle Knoten zu entfernen.

6. (Optional) Um die verfügbaren Knoten basierend auf einer Gemeinsamkeit zu filtern, legen Sie im Feld "Knotennamenfilter" einen Filterwert fest.

   Hinweis: Das Feld "Filter" unterstützt die Verwendung von Platzhalterzeichen.

   Acc* lässt Sie beispielsweise alle Knoten filtern, die einen Knotennamen haben, der mit "Acc." beginnt. Um die Filterergebnisse zu löschen, klicken Sie im Feld "Filter" auf X.

7. Klicken Sie auf "OK".

Die Knotengruppe wird geändert.

Aktualisieren von vCenter- und ESX Server-Details

CA ARCserve Central Host-Based VM Backup lässt Sie vCenter- und ESX-Server-Details aktualisieren, die zuvor hinzugefügt wurden.

Gehen Sie wie folgt vor:

1. Blenden Sie im Fenster "Knoten" über die Menüleiste "Gruppen" "vCenter/ESX-Gruppen" ein.
2. Wählen Sie die vCenter/ESX-Gruppe aus, für die Sie die Serverdetails aktualisieren wollen, klicken Sie mit der rechten Maustaste und klicken Sie dann auf "vCenter/ESX aktualisieren".

   Das Dialogfeld "vCenter/ESX aktualisieren" wird geöffnet.

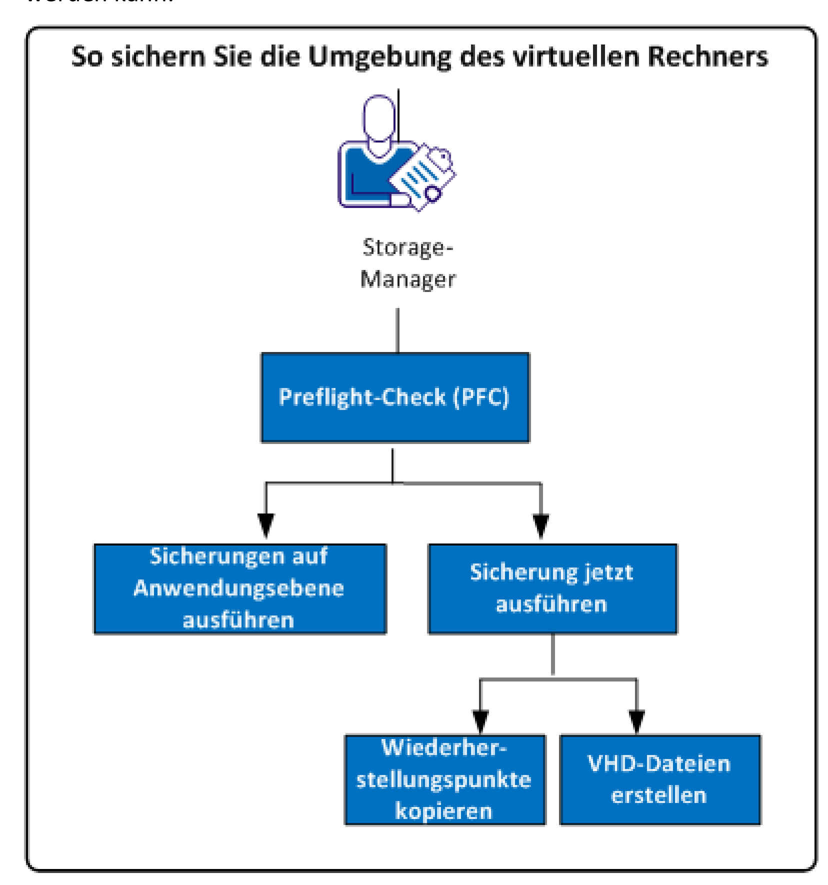
3. Aktualisieren Sie die Details des vCenter/ESX-Servers entsprechend.
4. Klicken Sie auf "OK".

   Das Dialogfeld "vCenter/ESX aktualisieren" schließt sich und die Knotengruppe ist aktualisiert.

Sichern der virtuellen Rechnerumgebung

Dieses Szenario erklärt, wie ein Speicheradministrator alle virtuellen Rechner in Ihrer Umgebung sichern und schützen kann.

Das folgende Diagramm veranschaulicht, wie die virtuelle Rechnerumgebung gesichert werden kann.



Die folgende Liste beschreibt die Prozesse, die im Diagramm veranschaulicht werden:

- Durchführen von Preflight-Checks für Ihre Sicherungsjobs (siehe Seite 62)
- Sicherung jetzt ausführen (siehe Seite 67)
  - Kopieren von Sicherungswiederherstellungspunkten (siehe Seite 70)
  - Erstellen von VHD-Dateien (siehe Seite 73)
- Durchführen von Sicherungen auf Anwendungsebene (siehe Seite 74)

Durchführen von Preflight-Checks für Ihre Sicherungsjobs

CA ARCserve Central Host-Based VM Backup enthält ein Hilfsprogramm namens Preflight-Check (PFC), das Ihnen ermöglicht, entscheidende Überprüfungen auf bestimmten Knoten auszuführen, um Bedingungen zu erkennen, die verursachen können, dass Sicherungsjobs fehlschlagen. Der Preflight-Check wird automatisch ausgeführt, wenn Sie die folgenden Aktionen ausführen:

- Importieren virtueller Rechner aus einem vCenter-/ESX-Serversystem
- Hinzufügen von Knoten vom Discovery-Ergebnis
- Aktualisieren von Knoten

Außerdem können Sie einen Preflight-Check auch manuell ausführen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Führen Sie eine der folgenden Aktionen aus, um die Knoten festzulegen, von denen aus Sie einen Preflight-Check ausführen wollen:

   - **Knotenebene**: Klicken Sie auf die Gruppe, die die Knoten enthält, von denen aus Sie einen Preflight-Check ausführen wollen, und aktivieren Sie das Kontrollkästchen neben dem Knoten. Klicken Sie dann mit der rechten Maustaste auf die Knoten und klicken Sie im Kontextmenü auf "Preflight-Check".
   - **Gruppenebene**: Klicken Sie mit der rechten Maustaste auf die Gruppe, die die Knoten enthält, und klicken Sie auf "Preflight-Check".

   Folgende Meldung wird angezeigt: "Preflight-Check des virtuellen Rechners wird gestartet."

3. Scrollen Sie zur Spalte "PFC-Status" und zeigen Sie den Status des Preflight-Checks an.

Die folgende Tabelle beschreibt die Überprüfungen, die vom Preflight-Check ausgeführt werden:

Element	Beschreibung
Verfolgung geänderter Blöcke (CBT)	CBT ist eine Funktion, die sich auf einem virtuellen Rechner befindende Datenträgersektoren nachverfolgt, die sich geändert haben. Dies hilft dabei, die Größe der Sicherungen zu minimieren. Dieses Element stellt sicher, dass CBT aktiviert ist.
VMware-Tools	Dieses Element stellt sicher, dass VMware Tools auf jedem virtuellen Rechner installiert sind.

Element	Beschreibung
Festplatte	Dieses Element überprüft die Datenträger des virtuellen Rechners.
Power-Status	Dieses Element stellt sicher, dass der virtuelle Rechner eingeschaltet ist.
Anmeldeinformationen	Dieses Element überprüft, ob die Benutzeranmeldeinformationen gültig sind.
Anwendungen	Dieses Element überprüft, ob Microsoft SQL Server und Microsoft Exchange Server installiert sind oder nicht.

Weitere Informationen dazu, wie Sie Fehler und Warnungen zu den Preflight-Check-Ergebnissen beheben können, finden Sie unter Lösungen für Preflight-Check-Elemente (siehe Seite 64).

Lösungen für Preflight-Check-Elemente

Die folgenden Tabellen beschreiben die Lösungen, die Ihnen dabei helfen, Fehler und Warnungen aus Ihren Preflight-Check-Ergebnissen zu beheben:

Verfolgung geänderter Blöcke (CBT)

Status	Meldung	Lösung
Warnung	"Verfolgung geänderter Blöcke" ist aktiviert, und Snapshots sind vorhanden. Eine vollständige Datenträgersicherung wird ausgeführt.	Um die verwendete Blocksicherung anzuwenden, führen Sie die folgenden Schritte aus: 1. Löschen Sie alle mit dem virtuellen Rechner verknüpften Snapshots. 2. Melden Sie sich am Host-Based VM Proxy-Server an. 3. Öffnen Sie den Registrierungs-Editor von Windows und suchen Sie nach dem folgenden Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFBackupDll\<VM-InstanzUUID> **Hinweis**: Ersetzen Sie <VM-InstanzUUID> durch den UUID-Wert des virtuellen Rechners, auf dem CBT fehlschlägt. Der Wert findet sich in der URL des virtuellen Rechners, die verwendet wird, wenn eine Verbindung mit CA ARCserve D2D hergestellt wird. 4. Setzen Sie den Registrierungsschlüssel auf "full disk backupForFullBackup"=0". 5. Erstellen/Setzen Sie die Registrierung auf ResetCBT=1. 6. Stellen Sie den Sicherungsjob in die Warteschlange.

VMware-Tools

Status	Meldung	Lösung
Warnung	Veraltet.	Installieren Sie die aktuelle Version von VMware-Tools.
Warnung	Nicht installiert oder nicht ausgeführt.	Installieren Sie die aktuelle Version von VMware-Tools und stellen Sie sicher, dass das Tool ausgeführt wird.

Festplatte

Status	Meldung	Lösung
Fehler	VM-Snapshots werden nicht für den virtuellen Rechner unterstützt, weil er über einen SCSI-Controller verfügt, der so konfiguriert ist, dass er sich einen Bus teilen kann.	Verwenden Sie CA ARCserve Central Protection Manager oder CA ARCserve D2D, um den virtuellen Rechner zu sichern.
Warnung	Der physische Raw Device Mapping-Datenträger (RDM) wird nicht gesichert.	Verwenden Sie CA ARCserve Central Protection Manager oder CA ARCserve D2D, um den virtuellen Rechner zu sichern.
Warnung	Die virtuelle Raw Device Mapping-Datenträger (RDM) wird als vollständiger Datenträger gesichert.	Verwenden Sie CA ARCserve Central Protection Manager oder CA ARCserve D2D, um den virtuellen Rechner zu sichern.
Warnung	Der unabhängige Datenträger wird nicht gesichert.	Verwenden Sie CA ARCserve Central Protection Manager oder CA ARCserve D2D, um den virtuellen Rechner zu sichern.
Warnung	Die Anwendung sichert den Datenträger im NFS-Datenspeicher als vollständigen Datenträger.	Verwenden Sie CA ARCserve Central Protection Manager oder CA ARCserve D2D, um den virtuellen Rechner zu sichern.

Power-Status

Status	Meldung	Lösung
Warnung	Ausgeschaltet	Starten Sie den virtuellen Rechner
Warnung	Unterbrochen	Starten Sie den virtuellen Rechner

Anmeldeinformationen

Status	Meldung	Lösung
Warnung	Inkorrekte Anmeldeinformationen.	Geben Sie gültige Benutzeranmeldeinformationen an.
Warnung	Nicht angegeben.	Geben Sie gültige Benutzeranmeldeinformationen an.

Anwendungen

Status	Meldung	Lösung
Warnung	Wiederherstellung auf Anwendungsebene wird nicht unterstützt, da die VM über IDE-Datenträger verfügt.	Verwenden Sie CA ARCserve Central Protection Manager oder CA ARCserve D2D, um Microsoft SQL Server- und Exchange Server-Daten zu sichern.
Warnung	VMware VIX ist nicht auf dem Hostserver installiert.	Laden Sie VIX von der VMware-Website herunter und installieren Sie es auf dem CA ARCserve Central Applications-Hostserver.
Warnung	VMware VIX auf dem CA ARCserve Central Host-Based VM Backup-Server ist veraltet.	Laden Sie VIX von der VMware-Website herunter und installieren Sie es auf dem CA ARCserve Central Applications-Hostserver.
Warnung	Wiederherstellung auf Anwendungsebene wird nicht unterstützt, da ESX Server nicht unterstützt wird.	Aktualisieren Sie ESX Server auf 4.1 oder höher oder verwenden Sie CA ARCserve Central Protection Manager oder CA ARCserve D2D, um Microsoft SQL Server- und Exchange Server-Daten zu sichern.
Warnung	Wiederherstellung auf Anwendungsebene wird nicht unterstützt, da nicht genügend SCSI-Slots verfügbar sind.	Verwenden Sie CA ARCserve Central Protection Manager oder CA ARCserve D2D, um Microsoft SQL Server- und Exchange Server-Daten zu sichern.
Warnung	Die Quelle befindet sich auf einem dynamischen Datenträger. Wiederherstellung auf Anwendungsebene wird nicht unterstützt.	Verwenden Sie CA ARCserve Central Protection Manager oder CA ARCserve D2D, um Microsoft SQL Server- und Exchange Server-Daten zu sichern. **Hinweis**: Auf virtuellen Rechnern, auf denen Windows Server 2008 oder höher mit dynamischen Datenträgern unter ESX-Server 4.1 oder höher ausgeführt wird, unterstützt VMware den inaktiven Modus auf Anwendungsebene nicht.
Warnung	Informationen zu der Anwendung konnten nicht abgerufen werden. Dies kann dazu führen, dass Sicherungen auf Anwendungsebene nicht erfolgreich abschließen.	Geben Sie die mitgelieferten Anmeldeinformationen oder die Anmeldeinformationen des Domänenadministrators an, um sich beim Gastbetriebssystem des virtuellen Rechners anzumelden. Aufgrund einer VMware-Beschränkung werden Sicherungen nur auf VMs unterstützt, die auf einem ESX-Server ausgeführt werden, für die eine bezahlte Lizenz vorliegt. Auf ESXi-Servern mit freier Lizenz werden Sicherungen nicht unterstützt.

Status	Meldung	Lösung
Warnung	Wiederherstellung auf Anwendungsebene wird auf Systemen mit aktivierten Speicherplätzen nicht unterstützt. Der virtuelle Rechner kann nur als Ganze wiederhergestellt werden.	Verwenden Sie CA ARCserve Central Protection Manager oder CA ARCserve D2D, um Microsoft SQL Server- und Microsoft Exchange Server-Daten zu sichern.

Sicherung jetzt ausführen

Normalerweise werden Ihre Sicherungen automatisch durchgeführt und von den Ablaufplan-Einstellungen gesteuert. Es können jedoch auch sofortige Ad-Hoc-Sicherungen (vollständige Sicherungen, Zuwachssicherungen oder Überprüfungssicherungen) erforderlich sein.

Eine Ad-Hoc-Sicherung wird eher nach Bedarf und nicht im Voraus als Teil eines Sicherungsplans geplant. Wenn Sie z. B. größere Veränderungen an Ihrem Rechner durchführen möchten, kann es sein, dass Sie sofort eine Ad-Hoc-Sicherung durchführen möchten, ohne abzuwarten, bis die geplanten Wiederholungsintervalle für vollständige Sicherungen, Zuwachssicherungen oder Überprüfungssicherungen abgelaufen sind.

Mit einer Ad-hoc-Sicherung können Sie einen benutzerdefinierten (ungeplanten) Wiederherstellungspunkt hinzuzufügen, sodass Sie bei Bedarf auf den Stand zu diesem Zeitpunkt zurückgreifen können. Wenn Sie z. B. einen Patch oder ein Service Pack installiert haben, das sich negativ auf die Leistung Ihres Rechners auswirkt, haben Sie die Möglichkeit, das System auf den Stand der Ad-Hoc-Sicherung vor dieser Installation zurückzusetzen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.
2. Klicken Sie in der Navigationsleiste der Startseite auf "Knoten", um die Ansicht "Knoten" zu öffnen.
3. Führen Sie eine der folgenden Aktionen aus, um die Knoten festzulegen, die Sie sichern wollen:
   - **Knotenebene:** Klicken Sie auf die Gruppe, die die Knoten enthält, die Sie sichern wollen, und aktivieren Sie die Kontrollkästchen neben den Knoten, die Sie sichern wollen.
   - **Gruppenebene:** Klicken Sie auf die Gruppe, die die Knoten enthält, die Sie sichern wollen.

4. Führen Sie eine der folgenden Aktionen aus, um den Knoten zu sichern:

   - Klicken Sie in der Symbolleiste auf "Sichern".
   - Klicken Sie mit der rechten Maustaste auf die ausgewählte Gruppe oder klicken Sie mit der rechten Maustaste auf die Knoten und klicken Sie im Kontextmenü auf "Jetzt sichern".

5. Legen Sie im Dialogfeld "Sicherung jetzt ausführen" einen Sicherungstyp fest, indem Sie auf einen der folgenden Typen klicken:

   - **Vollständige Sicherung:** Startet eine vollständige Sicherung Ihres gesamten Rechners oder des ausgewählten Volumes.
   - **Zuwachssicherung:** Startet eine Zuwachssicherung Ihres Rechners. Eine Zuwachssicherung sichert nur jene Blöcke, die seit der letzten Sicherung geändert wurden.

     Hinweis: Die Vorteile von Zuwachssicherungen bestehen darin, dass sie schnell durchgeführt werden und ein kleines Sicherungs-Image erstellen. Dies ist die optimale Methode zum Durchführen von Sicherungen.
   - **Überprüfungssicherung:** Startet eine Überprüfungssicherung Ihres Rechners, indem die aktuellste Sicherung von jedem einzelnen Block überprüft und der Inhalt und die Informationen mit der ursprünglichen Quelle verglichen wird. Dieser Vergleich stellt sicher, dass die letzten gesicherten Blöcke den jeweiligen Quellinformationen entsprechen. Wenn das Sicherungs-Image eines Blocks nicht der Quelle entspricht, aktualisiert CA ARCserve D2D die Sicherung dieses Blocks (Neusynchronisierung). Vergewissern Sie sich,dass Sie sich über die folgenden Vor- und Nachteile von Überprüfungssicherungen im Klaren sind:

     - Vorteile: Im Vergleich zu einer vollständigen Sicherung wird ein nur ein sehr kleines Sicherungs-Image erstellt, da nur die geänderten Blöcke (Blöcke, die nicht mit der letzten Sicherung übereinstimmen) gesichert werden.
     - Nachteile: Die Sicherung benötigt viel Zeit, da alle Blöcke des Quelldatenträgers mit den Blöcken der letzten Sicherung verglichen werden.

   Hinweis: Wenn Sie der Sicherungsquelle ein neues Volume hinzufügen, wird das neue Volume vollständig gesichert, unabhängig davon, welche allgemeine Sicherungsmethode ausgewählt wurde.

6. (Optional) Geben Sie einen Sicherungsnamen ein, und klicken Sie auf "OK". Wenn Sie keinen Namen angeben, wird die Sicherung standardmäßig Benutzerdefinierte/Vollständige/Zuwachs-/Überprüfungssicherung genannt.

Ein Bildschirm wird zur Bestätigung angezeigt, und der ausgewählte Sicherungstyp wird sofort gestartet.

Beachten Sie Folgendes:

- Alle in den Dialogfeldern der Richtlinien festgelegten Werte werden auf den Job angewendet.
- Wenn ein benutzerdefinierter Sicherungsjob (Ad-hoc) fehlschlägt, wird kein Ergänzungsjob erstellt. Ein Ergänzungsjob wird nur für geplante Jobs erstellt, die fehlschlagen.
- CA ARCserve Central Host-Based VM Backup wendet die folgenden Sicherungsjobs in Prioritätenfolge an:
  - Vollständige Sicherung
  - Überprüfen
  - Zuwachssicherung

  Die folgenden Bedingungen stellen sich ein, wenn ein "Jetzt sichern" übergeben wird und ein Job in der Warteschlange wartet:

  - Wenn eine vollständige Sicherung übergeben wird und ein Überprüfungssicherungsjob in der Warteschlange wartet, überschreibt die vollständige Sicherung den Job in der Warteschlange.
  - Wenn eine vollständige Sicherung übergeben wird und ein Zuwachsssicherungsjob in der Warteschlange wartet, überschreibt die vollständige Sicherung den Job in der Warteschlange.
  - Wenn eine Überprüfungssicherung übergeben wird und ein Zuwachsssicherungsjob in der Warteschlange wartet, überschreibt die Überprüfungssicherung den Job in der Warteschlange.
  - Wenn eine Überprüfungssicherung übergeben wird und eine vollständige Sicherung in der Warteschlange wartet, wird der Überprüfungssicherungsjob übersprungen.
  - Wenn eine Zuwachssicherung übergeben wird und eine vollständige Sicherung in der Warteschlange wartet, wird Zuwachssicherung übersprungen.
  - Wenn eine Zuwachssicherung übergeben wird und eine Überprüfungssicherung in der Warteschlange wartet, wird Zuwachssicherung übersprungen.

Kopieren von Wiederherstellungspunkten

Jedes Mal, wenn CA ARCserve D2D eine erfolgreiche Sicherung ausführt, wird gleichzeitig ein Snapshot-Image Ihrer Sicherung erstellt. Die so erfassten Wiederherstellungspunkte ermöglichen es Ihnen, ein zu kopierendes Sicherungs-Image zu suchen und auszuwählen. Sie können wie folgt vorgehen, um Ihre Sicherungen zu schützen:

- Kopieren/exportieren Sie Wiederherstellungspunktinformationen und speichern Sie sie an einem externen Ort, für den Fall, dass eine Katastrophe auftritt.
- Speichern Sie Ihre Wiederherstellungspunkte an verschiedenen Speicherorten.
- Zusätzlich können Sie Ihre Sicherungen konsolidieren, wenn das Sicherungsziel voll ist und Sie dennoch alle Wiederherstellungspunkte behalten möchten.

Wenn Sie einen Wiederherstellungspunkt auswählen, um ihn zu kopieren, erfassen Sie auch alle vorherigen Sicherungsblöcke, die benötigt werden, um ein vollständiges und aktuelles Sicherungs-Image wiederherzustellen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten mit den Wiederherstellungspunkten enthält, die Sie kopieren möchten.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

3. Suchen und klicken Sie auf den Knoten, auf dem Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

   CA ARCserve D2D wird geöffnet, und Sie werden auf der Startseite für den CA ARCserve D2D-Knoten angemeldet.

   Hinweis: Stellen Sie sicher, dass die Pop-up-Optionen in Ihrem Browser-Fenster aktiviert sind.

4. Wählen Sie auf der CA ARCserve D2D-Startseite "Wiederherstellungspunkt kopieren".

   Das Dialogfeld "Wiederherstellungspunkt kopieren" wird geöffnet.

5. Geben Sie im Feld "Speicherort für die Sicherung" die Sicherungsquelle an. Sie können den Speicherort der Sicherungs-Images angeben oder das System danach durchsuchen. Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen. Wenn erforderlich, müssen Sie Benutzernamen und Kennwort angeben, um Zugriff auf diesen Speicherort zu erhalten.

6. Klicken Sie im Feld "Virtueller Rechner" neben "Virtuellen Rechner auswählen" auf die Drop-down-Liste, um den virtuellen Rechner anzugeben, der die Wiederherstellungspunkte enthält, die Sie kopieren möchten.

   Im Kalender sind alle Daten für die angezeigte Zeitspanne, die Wiederherstellungspunkte für diese Sicherungsquelle enthalten, hervorgehoben.

7. Wählen Sie den zu kopierenden Wiederherstellungspunkt aus.

   a. Geben Sie das Datum des Sicherungs-Images an, das Sie wiederherstellen möchten.

      Es werden die entsprechenden Wiederherstellungspunkte einschließlich Uhrzeit, Sicherungstyp und Name der Sicherung angezeigt.

      Hinweis: Eine Uhr mit einem Sperrsymbol zeigt an, dass der Wiederherstellungspunkt verschlüsselte Informationen enthält und ein Kennwort zur Wiederherstellung benötigt.

   b. Wählen Sie einen Wiederherstellungspunkt aus, den Sie kopieren möchten.

      Die entsprechenden Sicherungsinhalte (einschließlich Anwendungen) für diesen Wiederherstellungspunkt werden angezeigt.

8. Klicken Sie auf "Weiter".

   Das Dialogfeld für Wiederherstellungsoptionen wird geöffnet.

   Hinweis: Es gibt zwei Kennwortfelder in diesem Dialogfeld. Das Feld "Kennwort" wird für das Kennwort zur Entschlüsselung der Quellsitzung verwendet, und das Feld "Verschlüsselungskennwort" wird verwendet, um die Zielsitzung zu verschlüsseln.

   a. Wenn der exportierte Wiederherstellungspunkt zu einem früheren Zeitpunkt verschlüsselt wurde, ist ein Kennwort erforderlich.

      - Wenn der exportierte Wiederherstellungspunkt eine Sicherungssitzung des gleichen Rechners ist, der auch die Kopie des Wiederherstellungspunkts ausführt, wird das Verschlüsselungskennwort gespeichert und automatisch aufgefüllt.

      - Wenn der exportierte Wiederherstellungspunkt eine Sicherungssitzung eines anderen Rechners ist, ist ein Verschlüsselungskennwort erforderlich.

   b. Wählen Sie das Ziel aus.

      Sie können den Speicherort für den ausgewählten Wiederherstellungspunkt angeben oder das System danach durchsuchen. Klicken Sie auf das grüne Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen. Wenn erforderlich, geben Sie Benutzernamen und Kennwort ein.

c. Wählen Sie das auszuführende Komprimierungslevel aus.

Hinweis: Das ausgewählte Komprimierungslevel für die Sicherung ist vom Komprimierungslevel für die Kopie unabhängig. Wenn z. B im Sicherungsziel die Komprimierungsstufe "Standard" festgelegt ist, kann das Komprimierungslevel für den Kopierjob auf "Keine Komprimierung" oder "Maximale Komprimierung" geändert werden.

Eine Komprimierung wird durchgeführt, um den verwendeten Speicherplatz zu verringern, hat aber aufgrund der erhöhten CPU-Auslastung auch eine umgekehrte Auswirkung auf die Geschwindigkeit der Sicherung.

Es sind folgende Optionen verfügbar:

- **Keine Komprimierung**: Es wird keine Komprimierung durchgeführt. Die Dateien sind reine VHD-Dateien. Diese Option bedeutet niedrigste CPU-Auslastung (höchste Geschwindigkeit), aber auch höchste Speicherplatzverwendung für Ihr Sicherungs-Image.
- **Standard-Komprimierung**: Komprimierung wird bis zu einem gewissen Grad durchgeführt. Diese Option bietet ein Gleichgewicht zwischen CPU-Auslastung und verwendetem Speicherplatz. Diese Option entspricht der Standardeinstellung.
- **Maximale Komprimierung**: Es wird eine maximale Komprimierung durchgeführt. Diese Option bedeutet höchste CPU-Auslastung (niedrigste Geschwindigkeit), aber auch niedrigste Speicherplatzverwendung für Ihr Sicherungs-Image.

Stellen Sie sich folgende Fragen:

- Wenn Ihr Sicherungs-Image unkomprimierbare Daten enthält (wie JPG-Images, ZIP-Dateien), wird zusätzlicher Speicherplatz verwendet, um diese Art von Daten zu verarbeiten. Die Aktivierung einer Komprimierungs-Option kann in solchen Fällen eine erhöhte Speicherplatzverwendung zur Folge haben.
- Wenn Sie die Komprimierungsstufe von "Keine Komprimierung" auf entweder "Standard-Komprimierung" oder "Maximale Komprimierung" ändern, oder wenn Sie von "Standard-Komprimierung" bzw. "Maximale Komprimierung" auf "Keine Komprimierung" wechseln, ist die erste Sicherung nach der Änderung der Komprimierungsstufe automatisch eine vollständige Sicherung. Nachdem diese vollständige Sicherung durchgeführt wurde, werden alle weiteren Sicherungen (vollständige Sicherung, Zuwachssicherung oder Überprüfungssicherung) gemäß dem Ablaufplan durchgeführt.

d. Wenn Sie möchten, dass der kopierte Wiederherstellungspunkt auch verschlüsselt wird, geben Sie folgende Informationen ein:

   Sie können Verschlüsselung für den kopierten Wiederherstellungspunkt ändern, hinzufügen oder entfernen.

   - Wählen Sie den Typ des Verschlüsselungsalgorithmus aus, der für die Kopie verwendet werden soll.

     Die verfügbaren Formatoptionen sind "Keine Verschlüsselung", "AES-128", "AES-192" und "AES-256".

   - Geben Sie ein Verschlüsselungskennwort an (und bestätigen Sie es).

9. Klicken Sie auf "Kopie erstellen".

   Ein Fenster zur Statusbenachrichtigung wird angezeigt, und der Kopiervorgang des ausgewählten Wiederherstellungspunkttyps wird umgehend gestartet.

   Hinweis: CA ARCserve D2D kann nur einen Kopierjob von Wiederherstellungspunkten zur gleichen Zeit ausführen.

   Das Image des Wiederherstellungspunktes wird von der Sicherungsquelle auf das Kopierziel kopiert.

Erstellen von VHD-Dateien in CA ARCserve Central Host-Based VM Backup

Dieser CA ARCserve D2D-Vorgang ermöglicht es Ihnen, eine "Virtual Hard Disk"-Datei (VHD) vom Wiederherstellungspunkt zu erstellen, der nach jeder erfolgreichen Sicherung erstellt wird. Weitere Informationen finden Sie im CA ARCserve D2D-Anhang.

Gehen Sie wie folgt vor:

1. Führen Sie die Schritte zu Wiederherstellungspunkte kopieren (siehe Seite 70) aus.
2. Wenn die Kopie fertig gestellt wird, durchsuchen Sie das angegebene Ziel, und navigieren Sie zum CA ARCserve D2D-Host.
3. Öffnen Sie den Ordner "VStore\S0000000001".
4. Suchen Sie alle Dateien mit der Erweiterung ".D2D" und ändern Sie sie in ".VHD". Nachdem Sie alle Dateien umbenannt haben, können sie als normale VHD-Dateien verwendet werden.

Durchführen von Sicherungen auf Anwendungsebene

Im Allgemeinen gibt es keine besonderen Schritte, die erforderlich sind, um Microsoft Exchange- oder SQL Server-Systeme zu schützen.

Um eine vollständige Anwendungssicherung auszuführen, stellen Sie sicher, dass die folgenden Punkte bestätigt sind:

- Alle Anwendungs-Writer sind in einem stabilen Zustand. Verwenden Sie *vssadmin*, um den Writer-Status anzuzeigen.
- Alle Datenbanken, die gesichert wurden, befinden sich in einem fehlerfreien Zustand. Stellen Sie beispielsweise bei SQL Server sicher, dass der Datenbankstatus nicht *Wird wiederhergestellt* ist.

Sie können auch Transaktionsprotokolle für SQL und Exchange Server separat abschneiden.

Hinweis: Wenn Sie ein Upgrade eines ESX-Servers durchführen, sollten Sie auch ein Upgrade von VMware Tools im Gastbetriebssystem vornehmen, bevor Sie Sicherungen auf Anwendungsebene durchführen, um Fehler aufgrund von veralteten Elementen zu vermeiden.

Ausführen vollständiger Datenträgersicherungen, die nur verwendete Blockdaten enthalten

Das Abrufen verwendeter Blockdaten nach Ausführen einer vollständigen Datenträgersicherung trägt dazu bei, das Sicherungsfenster zu reduzieren, und benötigt weniger Platz auf dem Sicherungsziel.

Hinweis: Aufgrund von VMware-Beschränkung können verwendete Blöcke nicht von virtuellen Rechnern abgerufen werden, wenn Wiederherstellungspunkt-Snapshots vorhanden sind. In solchen Fällen wird eine vollständige Datenträgersicherung auf dem virtuellen Rechner ausgeführt.

Nachdem eine vollständige Datenträgersicherung übergeben worden ist, führen Sie die folgenden Schritte aus, um die verwendeten Blockdaten abzurufen:

1. Löschen Sie alle mit dem virtuellen Rechner verknüpften Snapshots.
2. Melden Sie sich beim virtuellen CA ARCserve Central Host-Based VM Backup-Rechner an.
3. Öffnen Sie den Registrierungs-Editor von Windows und suchen Sie nach dem folgenden Schlüssel:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFBackupDll\VM_InstanceUUID
   ```
4. Legen Sie den Registrierungsschlüssel "full disk backupForFullBackup" auf 0 fest.
5. Erstellen Sie die Registrierung "ResetCBT" oder legen Sie sie fest auf 1.
6. Stellen Sie den Sicherungsjob in die Warteschlange.

Anzeigen von Jobstatusinformationen

CA ARCserve Central Virtual Standby konvertiert CA ARCserve D2D-Wiederherstellungspunkte in Wiederherstellungspunkt-Snapshots. Sie können Statusinformationen über sich in Bearbeitung befindende Host-Based VM Backup-Jobs anzeigen.

Wenn ein Job ausgeführt wird, können Sie detaillierte Informationen über den Job anzeigen. Sie können den aktuellen Job auch anhalten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.
2. Klicken Sie in der Navigationsleiste auf "Knoten", um die Ansicht "Knoten" zu öffnen.

3. Wenn sich in Bearbeitung befindende Host-Based VM Backup-Jobs vorliegen, wird die Phase des Jobs im Feld "Job" angezeigt, wie im folgenden Fenster veranschaulicht:



4. Klicken Sie auf die Phase, um das Dialogfeld "Statusüberwachung der Sicherung" zu öffnen.

   Hinweis: Weitere Informationen zu den Feldern, die in "Statusüberwachung der Sicherung" angezeigt werden, erhalten Sie unter Statusüberwachung der Sicherung. (siehe Seite 76)

5. Führen Sie eine der folgenden Optionen aus:

   - Klicken Sie auf "Schließen", um das Dialogfeld "Statusüberwachung der Sicherung" zu schließen.
   - Klicken Sie auf "Abbrechen", um den aktuellen Job anzuhalten.

     Hinweis: Das Dialogfeld "Statusüberwachung der Sicherung" schließt sich kurz nachdem Sie auf "Abbrechen" geklickt haben.

Weitere Informationen:

Anzeigen von Jobstatusinformationen (siehe Seite 75)

Überwachungsaufgaben von Host-Based VM Backup

Sie können den Status der Sicherungen Ihrer virtuellen Rechner im Fenster "Knoten" anzeigen. Suchen Sie über das Feld "Job" nach dem Knoten, der über einen sich in Bearbeitung befindenden Job verfügt und klicken Sie auf die Verknüpfung. Das Dialogfeld öffnet sich.

Sicherungen virtueller Rechner werden in zwei Phasen ausgeführt. Zuerst werden die virtuellen Festplatten gesichert. Wenn dies erfolgreich ist, wird der Katalog generiert. Der Katalog ermöglicht es Ihnen, Dateien und Ordner wiederherzustellen, oder den ganzen virtuellen Rechner.

Der Überwachungsserver zeigt die folgenden Echtzeitinformationen über den Sicherungsstatusjob an:

- **Phase (Sicherungs- und Katalogüberwachung)**: Zeigt den aktuellen Stand des Prozesses als schattierten Abschnitt des Fortschrittsbalkens an.
- **Startzeit (Sicherungs- und Katalogüberwachung)**: Zeigt das Datum und die Uhrzeit an, an dem der Sicherungsvorgang basierend auf der Richtlinienkonfiguration gestartet wurde.
- **Vergangene Zeit (Sicherungs- und Katalogüberwachung)**: Zeigt die Differenz zwischen der Startzeit und der aktuellen Zeit an.

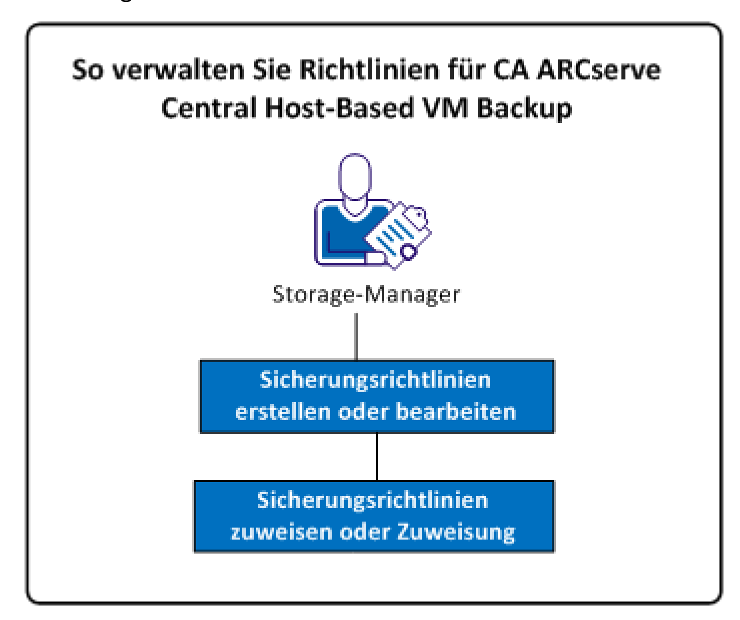
- **Geschätzte verbleibende Zeit (Nur Sicherungsüberwachung)**: Zeigt die geschätzte Zeit bis zum Abschluss des Jobs an.
- **Verarbeitung**:**(Nur Katalogüberwachung)** Zeigt den Laufwerksbuchstaben des Volumes oder die Anwendung an, für die gerade ein Katalog generiert wird.
- **Durch Komprimierung eingesparter Speicherplatz (Nur Sicherungsüberwachung)**: Zeigt den Teil des Festplattenspeichers an, der eingespart wird, wenn in der Sicherungsrichtlinie Komprimierung ausgewählt wurde.
- **Komprimierungsstufe**: **(Nur Sicherungsüberwachung)** Zeigt den Typ der Komprimierung an, die für Sicherungen verwendet wird. Die Optionen können "Keine Komprimierung", "Standard-Komprimierung" (Standard) oder "Maximale Komprimierung" sein.
- **Verschlüsselung (Nur Sicherungsüberwachung)**: Zeigt die Verschlüsselungsmethode an, die bei der Konfiguration des Sicherungsjobs ausgewählt wurde.
- **Schreibgeschwindigkeitslimit (Nur Sicherungsüberwachung)**: Zeigt den entsprechenden Wert an, wenn im Fenster "Schutzeinstellungen" der Sicherungsrichtlinie "Sicherung drosseln" festgelegt wurde.
- **Schreibgeschwindigkeit (Nur Sicherungsüberwachung)**: Zeigt die tatsächliche Schreibgeschwindigkeit in Megabyte pro Minute an.
- **Lesegeschwindigkeit (Nur Sicherungsüberwachung)**: Zeigt die tatsächliche Lesegeschwindigkeit in Megabyte pro Minute an.

So verwalten Sie Richtlinien für CA ARCserve Central Host-Based VM Backup

Sicherungsrichtlinien bestimmen, wie und wann Sie Knoten sichern sollten, die aus dem vCenter/ESX-Server importiert wurden. Speichermanager können Sicherungsrichtlinien erstellen und bearbeiten und dann Knoten zuweisen bzw. die Knotenzuweisung wieder aufheben.

Hinweis: Sie können eine Richtlinie einem oder mehreren Knoten zuweisen. Allerdings können Sie nicht eine oder mehrere Richtlinien einem Knoten zuweisen.

Das folgende Diagramm veranschaulicht den Prozess des Verwaltens von Sicherungsrichtlinien.



Die folgende Liste beschreibt die Prozesse, die im Diagramm veranschaulicht werden:

- Erstellen von Sicherungsrichtlinien (siehe Seite 79)
- Bearbeiten der Sicherungsrichtlinien (siehe Seite 83)
- Zuweisen und Aufheben der Zuweisung von Knoten aus Sicherungsrichtlinien (siehe Seite 86)

Erstellen von Sicherungsrichtlinien

Der Prozess zur Erstellung von Sicherungsrichtlinien verwendet in leicht veränderter Form die CA ARCserve D2D-Benutzeroberfläche, um Sicherungseinstellungen zu konfigurieren. Sie können Richtlinien erstellen, die auf ähnlichen Sicherungsbedürfnissen basieren, beispielsweise nach installierter Anwendung oder nach Ablaufplan.

Der folgende Vorgang fasst die Schritte zusammen, die für das Erstellen einer einfachen Richtlinie für CA ARCserve D2D-Sicherungsjobs erforderlich sind. Weitere Informationen zum Erstellen von CA ARCserve D2D-Sicherungsrichtlinien finden Sie im Anhang unter den entsprechenden CA ARCserve D2D-Themen.

Hinweis: Während einer hostbasierten Sicherung wird folgende Meldung angezeigt, wenn Sie Hotadd als Transportmodus verwenden:

```
Sie müssen den Datenträger in Laufwerk <Laufwerksbuchstabe> formatieren, bevor Sie
ihn verwenden können. Möchten Sie den Datenträger formatieren?
```

Klicken Sie auf "Abbrechen", um diese Meldung zu ignorieren. Die Meldung tritt auf, wenn das Betriebssystem erkennt, dass die virtuelle Festplatte zum Sicherungs-Proxy-Server hinzugefügt wurde. Das Betriebssystem geht davon aus, dass die virtuelle Festplatte ein neues Gerät ist, das Formatierung benötigt. Wenn Sie aus Versehen auf "Datenträger formatieren" klicken, tritt kein Fehler auf, da die virtuelle Festplatte schreibgeschützt ist.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Richtlinien", um die Ansicht "Richtlinien" zu öffnen.

2. Klicken Sie in der Symbolleiste auf "Neu", um das Dialogfeld "Neue Richtlinie" zu öffnen.

3. Geben Sie einen aussagekräftigen Richtliniennamen ein.

4. Klicken Sie auf der Registerkarte "Sicherungseinstellungen" auf "Schutzeinstellungen", und geben Sie folgende Informationen an:

   - **Sicherungsziel**: Geben Sie das lokale Volume oder den freigegebenen Remote-Ordner an, in dem Ihre Sicherungssitzungen gespeichert werden sollen.
   - **CA ARCserve D2D-VM-Sicherungs-Proxy**: Geben Sie den Hostnamen oder die IP-Adresse des Servers an, auf dem CA ARCserve D2D installiert wurde. Wenn CA ARCserve D2D noch nicht installiert wurde, können Sie CA ARCserve Central Protection Manager zur Bereitstellung verwenden. Geben Sie die entsprechenden Anmeldeinformationen für diesen Server an. Die Standardportnummer ist 8014. Wenn Sie während CA ARCserve D2D-Installation diesen Standard geändert haben, geben Sie die richtige Portnummer an.
   - **Aufbewahrungseinstellungen:** Sie können die Aufbewahrungsrichtlinie festlegen, die auf der Anzahl der aufzubewahrenden Wiederherstellungspunkte basiert (führt Sitzungen zusammen), oder die auf der Anzahl der aufzubewahrenden Wiederherstellungssätze basiert (löscht Wiederherstellungssätze und deaktiviert unendliche Zuwachssicherungen). Die Standardoption ist "Wiederherstellungspunkte aufbewahren". Weitere Details finden Sie im Kapitel "Festlegen der Schutzeinstellungen" des CA ARCserve Central Protection Manager-Benutzerhandbuchs.
   - **Komprimierung**: Wählen Sie eine Komprimierungsstufe aus. Der Standardwert ist "Standard-Komprimierung". Sie können "Keine Komprimierung" oder "Maximale Komprimierung" wählen.
   - **Verschlüsselung**: Geben Sie eine Verschlüsselungsebene an. Der Standardwert ist "Keine Verschlüsselung". Wenn Sie eine Verschlüsselungsebene auswählen, müssen Sie ein Verschlüsselungskennwort angeben, das zur Wiederherstellung von verschlüsselten Daten verwendet wird.
   - **Sicherung drosseln**: Geben Sie die Geschwindigkeit ein, in der Sicherungen auf den Datenträger geschrieben werden. Verkleinern Sie die Geschwindigkeit, um Netzwerk- oder CPU-Last reduzieren. Beachten Sie jedoch, dass dadurch die Sicherungszeiten vergrößert werden. Diese Option ist standardmäßig deaktiviert.

5. Klicken Sie auf "Ablaufplan", und füllen Sie folgende Felder aus:
   - **Startdatum und -zeit:** Geben Sie das Datum und den Zeitpunkt an, an dem Ihre Sicherungsjobs beginnen sollen.
   - **Zuwachssicherung**: Definieren Sie einen Wiederholungsablaufplan für Ihre Jobs zur Zuwachssicherung. Der Standardwert ist, Zuwachssicherungen einmal am Tag zu wiederholen.
   - **Vollständige Sicherung**: Definieren Sie einen Wiederholungsablaufplan für Ihre Jobs zur vollständigen Sicherung. Standardmäßig ist dieser Wert auf "Nie" eingestellt.
   - **Überprüfungssicherung**: Definieren Sie einen Wiederholungsablaufplan für die Jobs zur Überprüfungssicherung. Standardmäßig ist dieser Wert auf "Nie" eingestellt.
6. Klicken Sie auf "Erweitert", und geben Sie folgende Informationen ein:
   - **Protokoll abschneiden**: Aktivieren Sie die folgenden Optionen, wenn Sie Anwendungsprotokolldateien abschneiden möchten:
     - **SQL Server**: Wählen Sie einen täglichen, wöchentlichen oder monatlichen Ablaufplan zum Abschneiden aus.
     - **Exchange Server**: Wählen Sie einen täglichen, wöchentlichen oder monatlichen Ablaufplan zum Abschneiden aus.
   - **Speicherplatz auf Ziel reservieren**: Geben Sie den Prozentsatz des Speicherplatzes an, der für die Ausführung einer Sicherung reserviert werden soll. Dieser Betrag von kontinuierlichem Speicherplatz wird direkt vor dem Schreiben der Sicherung auf dem Ziel reserviert, was dabei hilft, die Sicherungsgeschwindigkeit zu verbessern.
   - **Kataloge**: Verwenden Sie die Option "Nach jeder Sicherung einen Dateisystemkatalog zur schnelleren Suche erstellen", um die Wartezeit für Browser-Suchen zu reduzieren.

     Wenn diese Option nicht aktiviert ist, können die Wiederherstellungen sofort nach der Sicherung ausgeführt werden, ohne warten zu müssen, bis der Katalogjob fertiggestellt ist. Standardmäßig ist diese Option deaktiviert. Beachten Sie Folgendes:
     - Wenn Sie für jeden Sicherungsjob einen Dateisystemkatalog generieren, resultiert dies in einem erhöhten erforderlichen Speicherplatz, um die Metadatendateien und Katalogdateien zu speichern, sowie zu einer erhöhten CPU-Auslastung. Wenn die Sicherungsquelle viele Dateien enthält, kann der Prozess, zur Kataloggenerierung außerdem eine zeitaufwändige Aufgabe sein.
     - Wenn Sie ReFS-Volumes als Sicherungsquelle auswählen, können keine Kataloge generiert werden. Es wird ein Warnhinweis angezeigt, der Sie über diesen Umstand informiert.

7. Klicken Sie auf "Einstellungen vor/nach Sicherung", und geben Sie gewünschte Befehle vor oder nach der Sicherung an. Geben Sie im Bedarfsfall die entsprechenden Anmeldeinformationen an:
   - **Befehl ausführen, bevor eine Sicherung gestartet wird**: Geben Sie den Skriptbefehl ein, der vor dem Start des Sicherungsjobs ausgeführt werden soll.
   - **Bei Beendigungscode**: Aktivieren Sie diese Option, wenn Sie den Skriptbefehl auf einem bestimmten Beendigungscode auslösen möchten.
   - **Job ausführen**: Legt fest, dass die Software den Job weiter ausführt, wenn der angegebene Beendigungscode zurückgegeben wird.
   - **Job abbrechen**: Legt fest, dass die Software den Sicherungsjob abbricht, wenn der angegebene Beendigungscode zurückgegeben wird.
   - **Befehl ausführen, nachdem ein Snapshot aufgenommen wurde**: Geben Sie den Skriptbefehl ein, der ausgeführt werden soll, nachdem der Snapshot aufgenommen wurde.
   - **Befehl ausführen, nachdem eine Sicherung abgeschlossen ist**: Geben Sie den Skriptbefehl ein, der ausgeführt werden soll, nachdem die Sicherung abgeschlossen wurde.
8. (Optional) Klicken Sie auf die Registerkarte "Voreinstellungen". Konfigurieren Sie je nach Bedarf eine der folgenden E-Mail-Warnungen:
   - Versäumte Jobs
   - vCenter/ESX nicht erreichbar (vor der Sicherung)
   - Lizenzfehler
   - Sicherungs-, Katalog-, Wiederherstellungs- oder Kopierjob fehlgeschlagen/abgestürzt/beendet
   - Sicherungs-, Katalog-, Wiederherstellungs- oder Kopierjob erfolgreich abgeschlossen
   - Freier Speicher am Ziel liegt unter dem folgenden Wert
   - Der Zusammenführungsjob wurde angehalten, übersprungen, schlug fehl oder ist abgestürzt
   - Zusammenführungsjob erfolgreich
   - Job in Jobwarteschlange überspringen/einfügen

Wenn Sie diese Optionen aktivieren, klicken Sie auf "E-Mail-Einstellungen", um Ihren E-Mail-Server zu konfigurieren. Geben Sie den Diensttyp, den Mailserver und den Port an. Wenn Authentifizierung erforderlich ist, aktivieren Sie diese Option, und geben Sie Anmeldeinformationen an.

- Geben Sie den Betreff an, der in der E-Mail angezeigt werden soll, zum Beispiel "CA ARCserve Central Host-Based VM Backup-Warnung".
- Geben Sie einen Wert für das Feld "Von" an, zum Beispiel "CA ARCserve Central Host-Based VM Backup".
- Geben Sie eine E-Mail-Adresse für alle Empfänger an. Trennen Sie die Adressen jeweils mit Strichpunkten (;) voneinander ab.

Sie können die Proxy-Einstellungen durch Angabe des Proxy-Servernamens, des Ports und der erforderlichen Anmeldeinformationen aktivieren.

Klicken Sie auf "OK".

9. Klicken Sie auf "Speichern".

Bearbeiten oder Kopieren von Sicherungsrichtlinien

Mit CA ARCserve Central Host-Based VM Backup können Sie CA ARCserve D2D-Sicherungsrichtlinien bearbeiten, nachdem sie erstellt wurden.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Richtlinien", um die Ansicht "Richtlinien" zu öffnen.

2. Klicken Sie im Fenster "Richtlinien" auf das Kontrollkästchen neben einer Richtlinie und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie in der Symbolleiste auf "Bearbeiten" und bearbeiten Sie die ausgewählte Richtlinie.
   - Klicken Sie in der Symbolleiste auf "Kopieren", um eine Richtlinie der ausgewählten Richtlinie zu kopieren und neu zu erstellen.

     Hinweis: Wenn Sie eine Richtlinie kopieren, öffnet sich das Dialogfeld "Richtlinie kopieren". Geben Sie einen Namen für die neue Richtlinie ein, und klicken Sie auf "OK".

   Das Dialogfeld "Richtlinie bearbeiten" wird geöffnet.

3. Wenn Sie den Namen der Richtlinie ändern wollen, geben Sie einen Namen im Feld "Richtliniennamen" an.

4. Klicken Sie auf der Registerkarte "Sicherungseinstellungen" auf "Schutzeinstellungen", und geben Sie folgende Informationen an:

   - **Sicherungsziel**: Geben Sie einen freigegebenen Remote-Ordner an, in dem Ihre Sicherungssitzungen gespeichert werden sollen.

   - **CA ARCserve D2D-VM-Sicherungs-Proxy**: Geben Sie den Hostnamen oder die IP-Adresse des Servers an, auf dem CA ARCserve D2D installiert wurde. Wenn CA ARCserve D2D noch nicht installiert wurde, können Sie CA ARCserve Central Protection Manager zur Bereitstellung verwenden. Geben Sie die entsprechenden Anmeldeinformationen für diesen Server an. Die Standardportnummer ist 8014. Wenn Sie während CA ARCserve D2D-Installation diesen Standard geändert haben, geben Sie die richtige Portnummer an.

   - **Aufbewahrungseinstellungen:** Sie können die Aufbewahrungsrichtlinie festlegen, die auf der Anzahl der aufzubewahrenden Wiederherstellungspunkte basiert (führt Sitzungen zusammen), oder die auf der Anzahl der aufzubewahrenden Wiederherstellungssätze basiert (löscht Wiederherstellungssätze und deaktiviert unendliche Zuwachssicherungen). Die Standardoption ist "Wiederherstellungspunkte aufbewahren". Weitere Details finden Sie im Kapitel "Festlegen der Schutzeinstellungen" des CA ARCserve Central Protection Manager-Benutzerhandbuchs.

   - **Komprimierung**: Wählen Sie eine Komprimierungsstufe aus. Der Standardwert ist "Standard-Komprimierung". Sie können "Keine Komprimierung" oder "Maximale Komprimierung" wählen.

   - **Verschlüsselung**: Geben Sie eine Verschlüsselungsebene an. Der Standardwert ist "Keine Verschlüsselung". Wenn Sie eine Verschlüsselungsebene auswählen, müssen Sie ein Verschlüsselungskennwort angeben, das zur Wiederherstellung von verschlüsselten Daten verwendet wird.

   - **Sicherung drosseln**: Geben Sie die Geschwindigkeit ein, in der Sicherungen auf den Datenträger geschrieben werden. Verkleinern Sie die Geschwindigkeit, um Netzwerk- oder CPU-Last reduzieren. Beachten Sie jedoch, dass dadurch die Sicherungszeiten vergrößert werden. Diese Option ist standardmäßig deaktiviert.

5. Klicken Sie auf "Ablaufplan", und füllen Sie folgende Felder aus:
   - **Startdatum und -zeit:** Geben Sie das Datum und den Zeitpunkt an, an dem Ihre Sicherungsjobs beginnen sollen.
   - **Zuwachssicherung**: Definieren Sie einen Wiederholungsablaufplan für Ihre Jobs zur Zuwachssicherung. Der Standardwert ist, Zuwachssicherungen einmal am Tag zu wiederholen.
   - **Vollständige Sicherung**: Definieren Sie einen Wiederholungsablaufplan für Ihre Jobs zur vollständigen Sicherung. Standardmäßig ist dieser Wert auf "Nie" eingestellt.
   - **Überprüfungssicherung**: Definieren Sie einen Wiederholungsablaufplan für die Jobs zur Überprüfungssicherung. Standardmäßig ist dieser Wert auf "Nie" eingestellt.
6. Klicken Sie auf "Erweitert", und geben Sie folgende Informationen ein:
   - **Protokoll abschneiden**: Aktivieren Sie die folgenden Optionen, wenn Sie Anwendungsprotokolldateien abschneiden möchten:
     - **SQL Server**: Wählen Sie einen täglichen, wöchentlichen oder monatlichen Ablaufplan zum Abschneiden aus.
     - **Exchange Server**: Wählen Sie einen täglichen, wöchentlichen oder monatlichen Ablaufplan zum Abschneiden aus.
   - **Speicherplatz auf Ziel reservieren**: Geben Sie den Prozentsatz des Speicherplatzes an, der für die Ausführung einer Sicherung reserviert werden soll. Dieser Betrag von kontinuierlichem Speicherplatz wird direkt vor dem Schreiben der Sicherung auf dem Ziel reserviert, was dabei hilft, die Sicherungsgeschwindigkeit zu verbessern.
   - **Kataloge**: Verwenden Sie die Option "Nach jeder Sicherung einen Dateisystemkatalog zur schnelleren Suche erstellen", um die Wartezeit für Browser-Suchen zu reduzieren.

     Wenn diese Option nicht aktiviert ist, können die Wiederherstellungen sofort nach der Sicherung ausgeführt werden, ohne warten zu müssen, bis der Katalogjob fertiggestellt ist. Standardmäßig ist diese Option deaktiviert.

     Hinweis: Wenn Sie für jeden Sicherungsjob einen Dateisystemkatalog generieren, resultiert dies in einem erhöhten erforderlichen Speicherplatz, um die Metadatendateien und Katalogdateien zu speichern, sowie zu einer erhöhten CPU-Auslastung. Wenn die Sicherungsquelle viele Dateien enthält, kann der Prozess, zur Kataloggenerierung außerdem eine zeitaufwändige Aufgabe sein.

     Hinweis: Wenn Sie ein ReFS-Volume oder ein dedupliziertes NTFS-Volume als die Sicherungsquelle ausgewählt haben, kann kein Katalog generiert werden, und es wird eine Warnmeldung angezeigt, die Sie über diese Bedingung informiert.

7. Klicken Sie auf "Einstellungen vor/nach Sicherung", und geben Sie erforderliche Befehle vor oder nach der Sicherung an. Geben Sie im Bedarfsfall die entsprechenden Anmeldeinformationen an:
   - **Befehl ausführen, bevor eine Sicherung gestartet wird**: Geben Sie den Skriptbefehl ein, der vor dem Start des Sicherungsjobs ausgeführt werden soll.
   - **Bei Beendigungscode**: Aktivieren Sie diese Option, wenn Sie den Skriptbefehl auf einem bestimmten Beendigungscode auslösen möchten.
   - **Job ausführen**: Legt fest, dass die Software den Job weiter ausführt, wenn der angegebene Beendigungscode zurückgegeben wird.
   - **Job abbrechen**: Legt fest, dass die Software den Sicherungsjob abbricht, wenn der angegebene Beendigungscode zurückgegeben wird.
   - **Befehl ausführen, nachdem ein Snapshot aufgenommen wurde**: Geben Sie den Skriptbefehl ein, der ausgeführt werden soll, nachdem der Snapshot aufgenommen wurde.
   - **Befehl ausführen, nachdem eine Sicherung abgeschlossen ist**: Geben Sie den Skriptbefehl ein, der ausgeführt werden soll, nachdem die Sicherung abgeschlossen wurde.
8. (Optional) Klicken Sie auf die Registerkarte "Voreinstellungen". Konfigurieren Sie nach Bedarf die gewünschten E-Mail-Warnmeldungen. Wenn Sie diese Optionen aktivieren, klicken Sie auf "E-Mail-Einstellungen", um Ihren E-Mail-Server zu konfigurieren.
9. Klicken Sie auf "Speichern".

Die Richtlinie wurde bearbeitet oder kopiert.

Zuweisen und Aufheben der Zuweisung von Knoten aus Sicherungsrichtlinien

Um mehrere virtuelle Rechner zu schützen, wählen Sie die Richtlinie aus, die Sie verwenden möchten, und weisen Sie sie einem oder mehreren Knoten zu.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an.

   Klicken Sie in der Navigationsleiste auf "Richtlinien", um die Ansicht "Richtlinien" zu öffnen.
2. Klicken Sie im Fenster "Richtlinien" auf die Registerkarte "Richtlinienzuweisung".
3. Wählen Sie aus der Richtlinienliste die Richtlinie aus, die Sie zuweisen möchten.

   Klicken Sie auf "Zuweisen und Zuweisung aufheben", um "Zuweisung der Richtlinie durchführen/aufheben" zu öffnen.

4. Geben Sie folgende Felder im Dialogfeld "Zuweisung der Richtlinie durchführen/aufheben" an:

   - **Gruppe:** Ermöglicht es Ihnen, den Gruppennamen auszuwählen, der die Knoten enthält, die Sie zuweisen möchten.
   - **Knotennamenfilter:** Lässt Sie die verfügbaren Knoten basierend auf einer Gemeinsamkeit filtern.

     Hinweis: Das Feld "Knotenname" ermöglicht es Ihnen, Knoten mithilfe von Platzhalterzeichen zu filtern.

     Acc* lässt Sie beispielsweise alle Knoten filtern, die einen Knotennamen haben, der mit "Acc." beginnt. Um die Filterergebnisse zu löschen, klicken Sie im Feld "Filter" auf X.

5. Führen Sie eine der folgenden Aktionen aus:

   - **Zuweisen von Knoten zu Richtlinien:** Wählen Sie die Knoten aus, die Sie hinzufügen möchten, und klicken Sie auf den einzelnen Rechtspfeil.

     Die Knoten werden von der Liste "Verfügbare Knoten" in die Liste "Ausgewählte Knoten" verschoben.

     Hinweis: Um alle Knoten auszuwählen und zu verschieben, klicken Sie auf den doppelten Rechtspfeil.

   - **Zuweisung der Knoten zu den Richtlinien aufzuheben:** Wählen Sie die Knoten aus, deren Zuweisung Sie aufheben möchten, und klicken Sie auf den einzelnen Rechtspfeil.

     Die Knoten bewegen sich von der Liste "Ausgewählte Knoten" zur Liste "Verfügbare Knoten".

     Hinweis: Um alle Knoten auszuwählen und zu verschieben, klicken Sie auf den doppelten Linkspfeil.

   Klicken Sie auf "OK".

6. Geben Sie im Bedarfsfall einen globalen Benutzernamen und ein Kennwort an, und wenden Sie sie auf die ausgewählten Knoten an.

   Klicken Sie auf "OK".

   Die ausgewählten Knoten werden der Liste "Richtlinienzuweisung" mit dem Bereitstellungsstatus [Zugewiesen] "Ausstehend" hinzugefügt.

   Hinweis: Sie können den Bereitstellungsstatus auch auf dem Bildschirm "Knoten" anzeigen.

7. Klicken Sie auf "Jetzt bereitstellen", um die zugewiesene Richtlinie sofort auf die angegebenen Knoten zu übertragen. Verwenden Sie die Schaltfläche "Aktualisieren", um den Status zu aktualisieren.

Im Fenster "Knoten" zeigt der Status für die Knoten, die Sie in der Liste "Richtlinienzuweisung" angegeben haben, nun die zugewiesene Richtlinie in der Spalte "Richtlinie" an. Klicken Sie auf den Knotennamen, und klicken Sie auf "Anmeldung bei D2D", um den Status Ihrer Sicherungsjobs zu überprüfen.

Anzeigen von CA ARCserve Central Host-Based VM Backup-Protokollen

Das Anzeigeprotokoll enthält umfassende Informationen zu den Vorgängen, die von Ihrer Anwendung ausgeführt werden. Das Protokoll liefert einen Audit-Pfad für jeden ausgeführten Job (an erster Stelle werden die letzten Aktivitäten aufgelistet) und kann bei der Behebung von Fehlern hilfreich sein.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Startseite in der Navigationsleiste auf "Protokolle anzeigen".

   Das Fenster "Protokolle anzeigen" wird angezeigt.

2. Geben Sie in den Drop-down-Listen die Protokollinformationen an, die Sie anzeigen möchten.

   - **Schweregrad:** Diese Option lässt Sie den Schweregrad des Protokolls angeben, das Sie anzeigen möchten. Sie können folgende Schweregradoptionen angeben:

     - **Alle:** Mit dieser Option werden alle Protokolle unabhängig vom Schweregrad angezeigt.

     - **Informationen:** Mit dieser Option werden nur Protokolle angezeigt, die allgemeine Informationen beschreiben.

     - **Fehler:** Mit dieser Option werden nur Protokolle angezeigt, die schwerwiegende Fehler beschreiben, die aufgetreten sind.

     - **Warnungen:** Mit dieser Option werden nur Protokolle angezeigt, die Fehler mit Warnmeldungen angezeigt, die aufgetreten sind.

     - **Fehler und Warnungen:** Mit dieser Option werden nur schwerwiegende Fehler und Fehler mit Warnmeldungen angezeigt, die aufgetreten sind.

- **Module:** Diese Option lässt Sie das Modul festlegen, für das Sie Protokolle anzeigen möchten. Sie können folgende Moduloptionen angeben:
  - **Alle:** Mit dieser Option werden Protokolle zu allen Anwendungskomponenten angezeigt.
  - **Allgemein:** Mit dieser Option werden Protokolle zu allgemeinen Prozessen angezeigt.
  - **Knoten aus Discovery importieren**: Mit dieser Option werden Protokolle zu aus Auto Discovery importierten Knoten angezeigt.
  - **Knoten aus Hypervisor importieren**: Mit dieser Option werden Protokolle zu vom Hypervisor importierten Knoten angezeigt.
  - **Richtlinienverwaltung:** Mit dieser Option werden nur Protokolle zur Verwaltung von Richtlinien angezeigt.
  - **Aktualisierungen**: Mit dieser Option werden nur Protokolle zu Aktualisierungen der Anwendung angezeigt.
  - **Preflight-Check:** Mit dieser Option werden nur Protokolle angezeigt, die den Status "Preflight-Check" für jeden Knoten ausgeführt haben.
  - **VM-Sicherungsjobs übergeben:** Mit dieser Option werden nur Protokolle angezeigt, in denen Knoten für Sicherungsjobs virtueller Rechner übergeben wurden.
  - **Mehrere Knoten aktualisieren**: Mit dieser Option werden nur Protokolle zu gleichzeitigen Aktualisierungen mehrerer Knoten angezeigt.
  - **<caad>-Zusammenführungsjob**: Mit dieser Option werden nur Protokolle zu <caad>-Zusammenführungsjobs angezeigt.
- **Knotenname:** Mit dieser Option werden nur Protokolle zu einem spezifischen Knoten angezeigt.

  Hinweis: Dieses Feld unterstützt die Platzhalter '*' und '?'. Geben Sie zum Beispiel "lod*" ein, um alle Aktivitätsprotokolle für Computernamen zurückzugeben, die mit "lod" beginnen.

Hinweis: Die Optionen "Schweregrad", "Module" und "Knotennamen" können zusammen angewendet werden. Sie können beispielsweise Fehler (Schweregrad) anzeigen, die sich auf Aktualisierungen (Module) für Knoten X (Knotenname) beziehen.

Die Protokollanzeige basiert auf den festgelegten Anzeigeoptionen.

Hinweis: Die im Protokoll angezeigte Zeit basiert auf der Zeitzone des Datenbankservers Ihrer Anwendung.

Anzeigen von Aktivitätsprotokollinformationen für einen bestimmten Knoten

CA ARCserve Central Host-Based VM Backup ermöglicht es Ihnen, Aktivitätsprotokollinformationen für einen bestimmten CA ARCserve D2D-Knoten anzuzeigen. Das Aktivitätsprotokoll liefert einen Audit-Pfad für jeden ausgeführten Job (an erster Stelle werden die letzten Aktivitäten aufgelistet) und kann bei der Behebung von Fehlern hilfreich sein.

So zeigen Sie Aktivitätsprotokollinformationen für einen bestimmten Knoten an

1. Öffnen Sie die Anwendung und klicken Sie in der Navigationsleiste auf "Knoten".

   Der Bildschirm "Knoten" wird angezeigt.

2. Klicken Sie in der Gruppenliste auf "Alle Knoten" oder klicken Sie auf die Gruppe, die den CA ARCserve D2D-Knoten enthält, bei dem Sie sich anmelden wollen.

   Die Liste der Knoten zeigt alle Knoten an, die der angegebenen Gruppe zugeordnet sind.

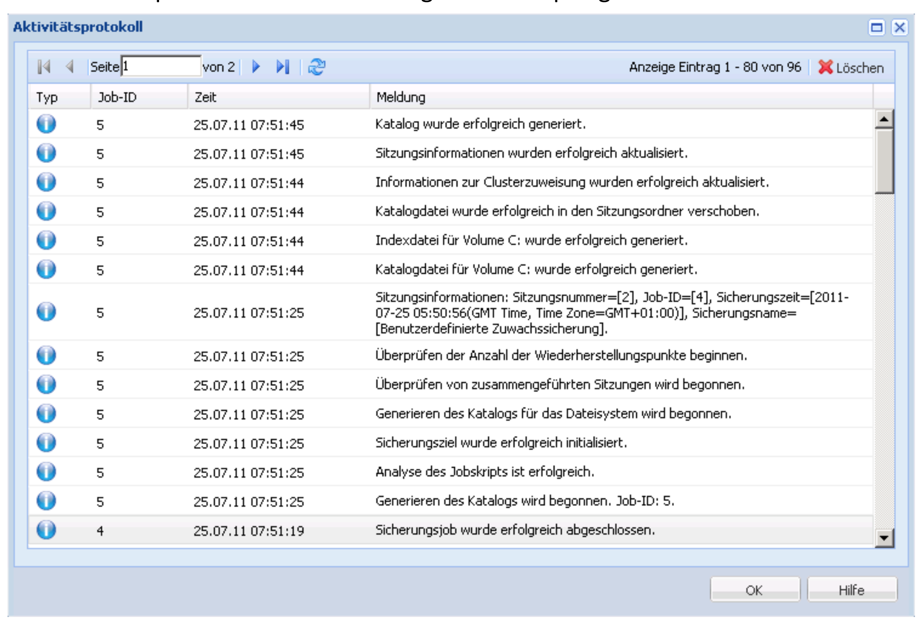
3. Suchen und klicken Sie auf den Knoten, auf dem Sie sich anmelden möchten, und klicken Sie anschließend im Pop-up-Menü auf "Anmeldung bei D2D".

   CA ARCserve D2D wird geöffnet, und Sie werden auf der Startseite für den CA ARCserve D2D-Knoten angemeldet.

   Hinweis: Wenn sich ein neues Browser-Fenster nicht öffnet, stellen Sie sicher, dass die Pop-up-Optionen für Ihren Browser alle Pop-up-Fenster oder Pop-up-Fenster nur auf dieser Website zulassen.

4. Klicken Sie in der Aufgabenliste auf "Protokolle anzeigen".

   Das Aktivitätsprotokoll wird wie im folgenden Beispiel geöffnet:



   Das Aktivitätsprotokoll stellt folgende Informationen bereit:

   - **Typ**: Gibt den Schweregrad der Aktivität an, die Informationen, Warnungen und Fehler erfasst.
   - **Job-ID**: Gibt den Job an, auf den sich die Aktivität bezieht.
   - **Zeit**: Gibt die Daten und Zeit an, auf die sich die Aktivität bezieht.
   - **Meldung:** Beschreibt die Aktivität.

5. Klicken Sie auf "OK", um das Aktivitätsprotokoll zu schließen.

CA ARCserve Central Host-Based VM Backup-Status in einem Bericht anzeigen

Wenn Sie CA ARCserve Central Protection Manager und CA ARCserve Central Reporting installiert haben, können Sie den hostbasierten VM-Sicherungs-Proxy-Server zu CA ARCserve Central Protection Manager hinzufügen und anschließend den Virtualisierungsschutz-Statusbericht erstellen, um den Status Ihres hostbasierten Sicherungsproxy anzuzeigen.

Weitere Informationen zum Virtualisierungsschutz-Statusbericht finden Sie im CA ARCserve Central Reporting-Benutzerhandbuch.

Links zur Navigationsleiste hinzufügen

Jedes des CA ARCserve Central Applications verfügt in der Navigationsleiste über den Link "Neue Registerkarte hinzufügen". Verwenden Sie diese Funktion, um in der Navigationsleiste Einträge für zusätzliche webbasierte Anwendungen hinzuzufügen, die Sie verwalten möchten. Für jede installierte Anwendung wird automatisch eine neue Verknüpfung zur Navigationsleiste hinzugefügt. Wenn Sie beispielsweise CA ARCserve Central Reporting und CA ARCserve Central Virtual Standby auf "Computer A" installiert haben und CA ARCserve Central Reporting starten, wird CA ARCserve Central Virtual Standby automatisch zur Navigationsleiste hinzugefügt.

Hinweis: Die neu installierten Anwendungen werden nur entdeckt, wenn sich auf demselben Computer eine andere CA ARCserve Central Applications-Anwendung befindet.

Gehen Sie wie folgt vor:

1. Klicken Sie in der Navigationsleiste der Anwendung auf den Link "Neue Registerkarte hinzufügen".
2. Geben Sie den Namen und die URL der Anwendung oder Website an, die Sie hinzufügen wollen. Zum Beispiel, www.google.com.

   Geben Sie optional den Speicherort eines Symbols an.
3. Klicken Sie auf "OK".

   Die neue Registerkarte wird dem unteren Ende der Navigationsleiste hinzugefügt.

Beachten Sie Folgendes:

- Die CA Support-Verknüpfung wird Ihnen standardmäßig zur Verfügung gestellt.

Sie können die neue Registerkarte entfernen, indem Sie sie markieren und auf "Entfernen" klicken.

Besondere Aspekte beim Schutz von Partitionsgerätzuordnungen

Berücksichtigen Sie folgendes Verhalten, wenn Partitionsgerätzuordnungen (RDM) geschützt werden:

- Die Anwendung unterstützt nicht den Schutz von Partitionsgerätzuordnungen im physischen kompatiblem Modus (Datenträger dieses Typs sind physische Geräte). Während des Sicherungsvorgangs lässt die Anwendung Partitionsgerätzuordnungen im physischen kompatiblem Modus von der Sicherungsquelle aus. Eine Lösung dieses Problems ist, CA ARCserve D2D unter einem Gastbetriebssystem zu installieren und Sicherungen auf dieselbe Art und Weise wie die Sicherung von physischen Datenträgern durchzuführen.

- Die Anwendung unterstützt den Schutz von Partitionsgerätzuordnungen im virtuellen Kompatibilitätsmodus. Beachten Sie jedoch folgende Einschränkungen:
  - In Bezug auf vollständige Sicherungen ermöglicht es Ihnen die Anwendung, vollständige RDM-Datenträger im virtuellen Kompatibilitätsmodus zu sichern. Wenn Sie Datenkomprimierung nicht verwenden, können die Sicherungsdatensätze dieselbe Größe wie der Quelldatenträger haben.
  - CA ARCserve Central Host-Based VM Backup stellt virtuelle RDM-Datenträger in Kompatibilitätsmodus als normale virtuelle Datenträger wieder her. Nachdem die Wiederherstellung abgeschlossen hat, ist der Datenträger nicht mehr als virtueller RDM-Datenträger konfiguriert. Auch verhält er sich nicht mehr als solcher.
  - Eine alternative Vorgehensweise zur Sicherung der RDMs im virtuellen Kompatibilitätsmodus ist es, CA ARCserve D2D unter einem Gastbetriebssystem zu installieren und die RDMs in derselben Art und Weise zu sichern, wie Sie physische Rechner sichern würden.

Ändern des Server-Kommunikationsprotokolls

CA ARCserve Central Applications verwendet standardmäßig Hypertext Transfer Protocol (HTTP) zur Kommunikation zwischen seinen Komponenten. Wenn Ihnen eine sichere Übertragung von Kennwörtern zwischen den Komponenten wichtig ist, wählen Sie das Protokoll Hypertext Transfer Protocol Secure (HTTPS). Wenn Sie dagegen diese zusätzliche Sicherheitsstufe nicht benötigen, können Sie das Protokoll ganz einfach wieder auf HTTP zurücksetzen.

Gehen Sie wie folgt vor:

1. Melden Sie sich über ein Administratorkonto oder ein Konto mit Administratorrechten bei dem Computer an, auf dem die Anwendung installiert ist.

   Hinweis: Wenn Sie sich nicht über ein Administratorkonto oder ein Konto mit Administratorrechten anmelden, konfigurieren Sie die Befehlszeile so, dass sie mit dem Recht "Als Administrator ausführen" ausgeführt wird.

2. Öffnen Sie die Windows-Befehlszeile.

3. Wählen Sie eine der folgenden Vorgehensweisen:

   - **So ändern Sie das Protokoll von HTTP auf HTTPS:**

     Starten Sie das Hilfsprogramm-Tool "changeToHttps.bat" von folgendem Standardspeicherort (der Speicherort des Ordners 'BIN' kann variieren, je nach dem, wo Sie die Anwendung installiert haben):

     ```
     C:\Programme\CA\ARCserve Central Applications\BIN
     ```

     Wenn das Protokoll erfolgreich geändert wurde, wird die folgende Meldung angezeigt:

     ```
     Das Kommunikationsprotokoll wurde auf HTTPS geändert.
     ```

   - **So ändern Sie das Protokoll von HTTPS auf HTTP:**

     Starten Sie das Hilfsprogramm-Tool "changeToHttp.bat" von folgendem Standardspeicherort (der Speicherort des Ordners 'BIN' kann variieren, je nach dem, wo Sie die Anwendung installiert haben):

     ```
     C:\Programme\CA\ARCserve Central Applications\BIN
     ```

     Wenn das Protokoll erfolgreich geändert wurde, wird die folgende Meldung angezeigt:

     ```
     Das Kommunikationsprotokoll wurde auf HTTP geändert.
     ```

4. Starten Sie den Browser neu und stellen Sie die Verbindung zu CA ARCserve Central Applications neu her.

   Hinweis: Wenn Sie das Protokoll auf HTTPS ändern, wird im Webbrowser eine Warnung angezeigt. Dieses Verhalten tritt wegen eines selbstsignierten Sicherheitszertifikats auf, das Sie auffordert, die Warnung zu ignorieren und fortzufahren, oder dieses Zertifikat zum Browser hinzuzufügen, um dieser Warnung künftig vorzubeugen.

Definieren eines Transportmodus für Sicherungen

Sie können einen bestimmten Transportmodus (Übertragungsdaten) definieren, der für D2D-Sicherungsjobs verwendet wird, die unter Host-Based VM Backup ausgeführt werden. Standardmäßig verwendet Host-based VM Backup einen Modus, der es Host-Based VM Backup erlaubt, die Leistung (durch Erhöhung der Geschwindigkeit) des Sicherungsvorgangs zu optimieren. Wenn Sie einen bestimmten Transportmodus für Sicherungen angeben wollen, konfigurieren Sie allerdings den in diesem Abschnitt beschriebenen Registrierungsschlüssel.

Host-Based VM Backup kann Sicherungen mithilfe der folgenden Transportmodi ausführen:

- HOTADD-Transportmodus (siehe Seite 211)
- NBD-Transportmodus (siehe Seite 211)
- NBDSSL-Transportmodus (siehe Seite 211)
- SAN-Transportmodus (siehe Seite 212)

Beachten Sie Folgendes:

- Dies ist eine optionale Konfigurationsaufgabe. Standardmäßig führt Host-Based VM Backup Sicherungen mithilfe eines Transportmodus aus, der die Leistung des Sicherungsvorgangs optimiert.
- Wenn Sie diesen Registrierungsschlüssel konfigurieren, um einen bestimmten Transportmodus zu verwenden, und der Modus nicht verfügbar ist, verwendet Host-Based VM Backup einen verfügbaren Standardtransportmodus für die Sicherung.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim CA ARCserve D2D-Sicherungs-Proxy-System für die virtuellen Rechner an.

   Öffnen Sie die Windows-Registrierung, und suchen Sie nach dem folgenden Registrierungsschlüssel:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE
   D2D\AFBackupDll\{VM-InstanceUUID}].
   ```

2. Klicken Sie mit der rechten Maustaste auf "VM-InstanceUUID", wählen Sie "Neu" aus und klicken Sie im Pop-up-Menü auf "Zeichenfolgewert".

   Nennen Sie den neuen Zeichenfolgenwert folgendermaßen:

   ```
   EnforceTransport
   ```

3. Klicken Sie mit der rechten Maustaste auf "EnforceTransport" und klicken Sie im Pop-up-Menü auf "Ändern", um das Dialogfeld "Zeichenfolge bearbeiten" zu öffnen.

4. Geben Sie im Feld "Wertdaten" den Transportmodus an, den Sie während des Sicherungsjobs verwenden wollen. Legen Sie einen der folgenden Werte fest:

   hotadd

   HOTADD-Transportmodus (siehe Seite 211)

   nbd

   NBD-Transportmodus (siehe Seite 211)

   nbdssl

   NBDSSL-Transportmodus (siehe Seite 211)

   SAN

   SAN-Transportmodus (siehe Seite 212)

5. Klicken Sie auf OK, um den Wert anzuwenden und das Dialogfeld "Zeichenfolge bearbeiten" zu schließen.

Der Transportmodus ist damit definiert und wird das nächste Mal, wenn ein Job ausgeführt wird, verwendet.

Kapitel 4: Wiederherstellen und Zurückgewinnen von virtuellen Rechnern

Die verfügbaren Optionen zur Wiederherstellung und Zurückgewinnung hängen davon ab, wie Ihr System gesichert wurde. Zum Beispiel können Sie keine mit CA ARCserve Central Host-Based VM Backup erstellten Sicherungssitzungen verwenden, um detaillierte Wiederherstellungen auf Anwendungsebene oder von Microsoft Exchange-Objekten auszuführen. Für diese Wiederherstellungen können Sie Sitzungen verwenden, die mit CA ARCserve Central Protection Manager oder CA ARCserve D2D erstellt wurden. Bestimmte in CA ARCserve D2D verfügbare Wiederherstellungsoptionen stehen möglicherweise in dieser Anwendung nicht zur Verfügung. Zum Beispiel ist "Am ursprünglichen Speicherort wiederherstellen" bei Sicherungen der Anwendung nicht möglich, da der Speicherort des Proxy-Servers nicht mit dem Speicherort des virtuellen Rechners der Sicherungsquelle übereinstimmt.

Konsultieren Sie Hinweise zur Wiederherstellung (siehe Seite 114), um zu bestimmen, welche der verfügbaren Wiederherstellungsmethoden (siehe Seite 100) in welchen Fällen angebracht sind.

Dieses Kapitel enthält folgende Themen:

Wiederherstellungsmethoden

Die Methode, die Sie zur Erstellung der Sicherungssitzung verwenden, bestimmt die verfügbaren Wiederherstellungsmethoden. So sind zum Beispiel einige Wiederherstellungsmethoden nur verfügbar, wenn dazu eine lokal installierte CA ARCserve D2D-Version verwendet wird. Für andere Methoden ist es erforderlich, den virtuellen Rechner zum Zeitpunkt der Sicherung einzuschalten.

Wiederherstellungspunkte durchsuchen **(siehe Seite 101)**

Ermöglicht es Ihnen, die verfügbaren Wiederherstellungspunkte (erfolgreiche Sicherungen) in einem Kalender zu suchen. Verwenden Sie diese Methode zur Wiederherstellung von Dateien und Ordnern oder zur Wiederherstellung auf Anwendungsebene.

Mit CA ARCserve D2D, CA ARCserve Central Host-Based VM Backup oder CA ARCserve Central Protection Manager erstellte Sicherungen können mit dieser Methode wiederhergestellt werden.

Wiederherzustellende Dateien/Ordner suchen **(siehe Seite 105)**

Ermöglicht es Ihnen, bestimmte wiederherzustellende Dateien oder Ordner zu suchen.

Mit CA ARCserve D2D erstellte Sicherungen können mit dieser Methode wiederhergestellt werden. Sicherungen, die mit CA ARCserve Central Host-Based VM Backup und CA ARCserve Central Protection Manager erstellt wurden, können auch wiederhergestellt werden, wenn der virtuelle Rechner zum Zeitpunkt der Sicherung eingeschaltet war.

VM wiederherstellen **(siehe Seite 108)**

Ermöglicht es Ihnen, alle verfügbaren Wiederherstellungspunkte von virtuellen Rechnern (erfolgreiche Sicherungen) in einem Kalender zu suchen. Sie können dann den virtuellen Rechner angeben, den Sie wiederherstellen möchten.

Diese Methode ist verfügbar, um Sicherungen, die mit CA ARCserve Central Host-Based VM Backup erstellt wurden, wiederherzustellen. Zuerst wird dabei ein virtueller Rechner bereitgestellt und danach das Betriebssystem, Anwendungen und Daten aus dem angegebenen Wiederherstellungspunkt wiederhergestellt.

Wiederherstellung auf Anwendungsebene **(siehe Seite 115)**

Um einen Microsoft Exchange Server oder SQL Server vollkommen wiederherzustellen, ohne ihn neu aufbauen zu müssen, klicken Sie in einer lokal installierten CA ARCserve D2D-Version auf die Methode "Wiederherstellungspunkte durchsuchen".

Bare-Metal-Recovery (siehe Seite 167)

Bare-Metal-Recovery (BMR) ist der Prozess zur Wiederherstellung eines Computer "von Null" an, einschließlich Betriebssystem, Software-Anwendungen, Einstellungen und Daten. Für eine BMR-Wiederherstellung ist es erforderlich, über ein Windows-Image oder ein Start-Kit und mindestens eine vollständige Sicherung zu verfügen. Mit CA ARCserve D2D, CA ARCserve Central Host-Based VM Backup, CA ARCserve Central Virtual Standby und CA ARCserve Central Protection Manager erstellte Sicherungen können mit dieser Methode wiederhergestellt werden. Wenn der virtuelle Rechner während der Sicherung ausgeschalten war, ist BMR allerdings nicht möglich.

Von Wiederherstellungspunkten aus wiederherstellen

Mit der Wiederherstellungsmethode "Wiederherstellungspunkte durchsuchen" können Sie erfolgreiche Sicherungen (Wiederherstellungspunkte genannt) in einem Kalender suchen. Sie können nach Sicherungsinhalt, einschließlich wiederherzustellende Anwendungen, suchen und eine Auswahl machen. Der Vorgang zur Wiederherstellung mit der Methode "Wiederherstellungspunkte durchsuchen" gleicht der Methode in CA ARCserve D2D bis auf eine Ausnahme. Zur Wiederherstellung von Wiederherstellungspunkten virtueller Rechner kann die Option "Am ursprünglichen Speicherort wiederherstellen" nicht verwendet werden.

Gehen Sie wie folgt vor:

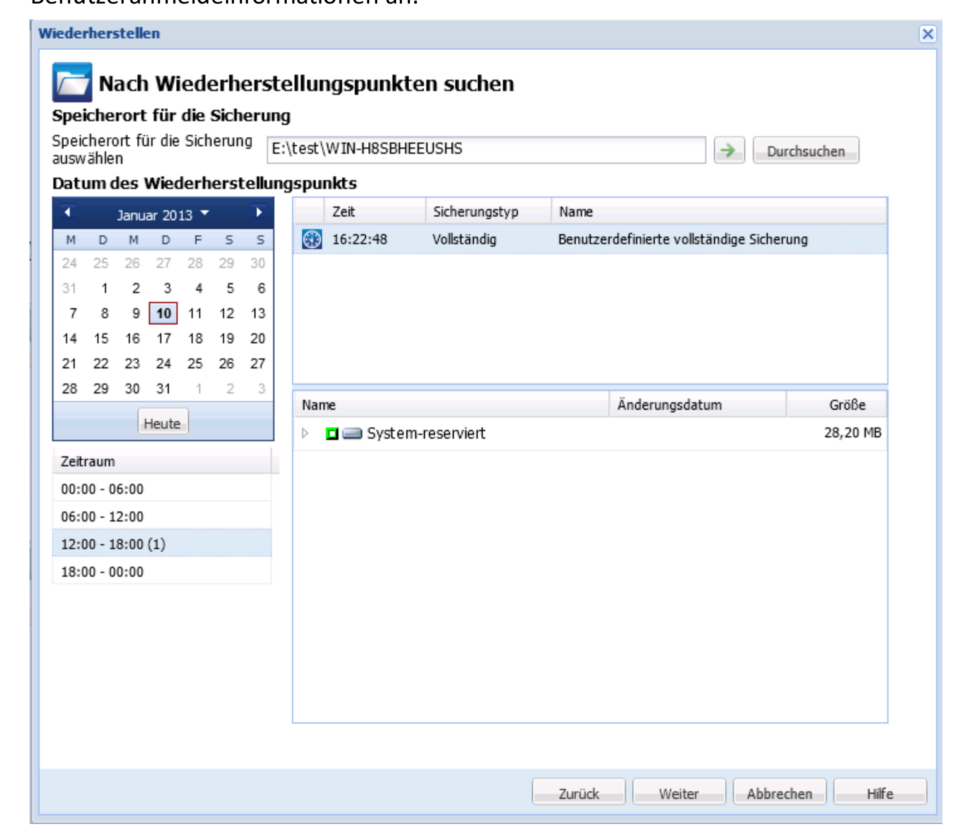
1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

   Blenden Sie im Fenster "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen möchten.

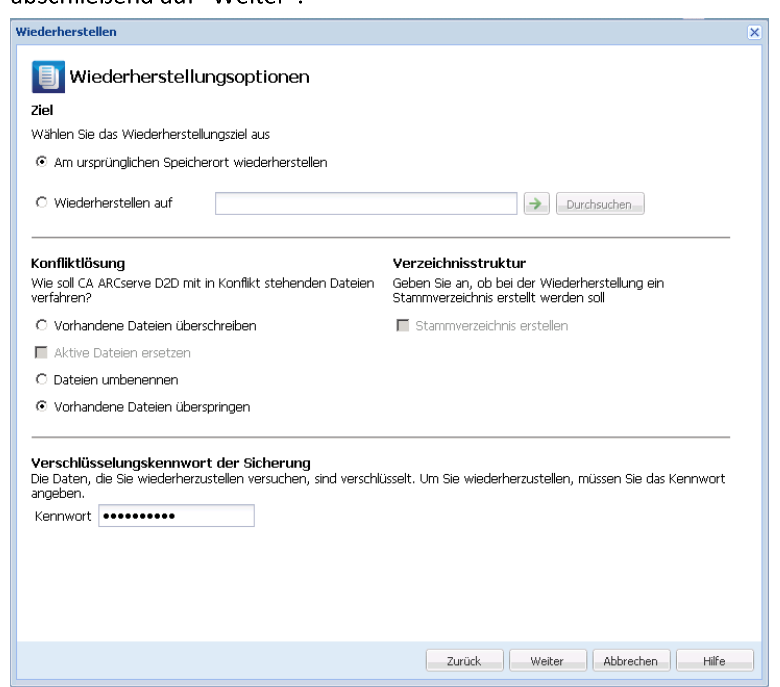
   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen möchten, und klicken Sie dann auf der Symbolleiste auf "Wiederherstellen".

2. Klicken Sie im Dialogfeld "Wiederherstellung" auf "Wiederherstellungspunkte durchsuchen".

   Das Dialogfeld "Wiederherstellen" wird geöffnet und der Speicherort für die Sicherung wird je nach ausgewähltem Knoten angegeben. Ändern Sie den Speicherort nach Bedarf auf ein anderes Sicherungsziel und geben Sie die Benutzeranmeldeinformationen an.



3. Klicken Sie auf das Datum des Wiederherstellungspunkts, und klicken Sie dann auf den Zeitpunkt der Wiederherstellung. Wählen Sie den wiederherzustellenden Inhalt aus. Wählen Sie ein ganzes Volume oder eine Datei, einen Ordner, eine Datenbank oder eine Anwendung aus. Ausgefüllte grüne Kästchen neben einer Auswahl zeigen an, dass dieses Element zur Wiederherstellung ausgewählt wurde. Klicken Sie abschließend auf "Weiter".



4. Geben Sie im Dialogfeld "Wiederherstellungsoptionen" das Wiederherstellungsziel an.

   - **Am ursprünglichen Speicherort wiederherstellen (deaktiviert)**: In CA ARCserve Central Host-Based VM Backup-Sitzungen können Sie keine Wiederherstellungen am ursprünglichen Speicherort durchführen. Um Dateien oder Ordner im Gast-BS einer VM an ihrem ursprünglichen Speicherort wiederherzustellen, müssen Sie entweder auf dem Gast-BS CA ARCserve D2D installieren oder die Wiederherstellung auf einem freigegebenen Netzwerkordner auf der VM durchführen.
   - **Wiederherstellen auf**: Geben Sie das gewünschte Wiederherstellungsziel an.
   - **Vorhandene Dateien überschreiben**: Ersetzt die Dateien des Zielspeicherorts.
   - **Aktive Dateien ersetzen**: Ersetzt derzeit verwendete Dateien oder Dateien, auf die bei einem Neustart zugegriffen wird.
   - **Dateien umbenennen**: Erstellt eine neue Datei, wenn der Dateiname bereits vorhanden ist. Mit dieser Option wird die Quelldatei mit dem gleichen Dateinamen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Daten werden in der Datei mit der neuen Erweiterung wiederhergestellt.
   - **Vorhandene Dateien überspringen**: Überspringt vorhandene Dateien, die am Wiederherstellungsziel gespeichert sind, und ersetzt die Dateien nicht. Dies ist die Standardeinstellung.
   - **Stammverzeichnis erstellen**: Erstellt am Ziel die gleiche Stammverzeichnisstruktur, die im Sicherungs-Image vorhanden ist.

5. Klicken Sie auf "Weiter". Überprüfen Sie im Fenster "Wiederherstellungs-Übersicht", ob alle Optionen korrekt angegeben wurden. Wenn nicht alle Einstellungen richtig sind, klicken Sie auf "Zurück". Wenn alle Einstellungen richtig sind, klicken Sie auf "Fertig stellen", um den Wiederherstellungsvorgang zu starten.

Wiederherstellung durch Laden eines Wiederherstellungspunkts

Die Wiederherstellung durch Laden eines Wiederherstellungspunkts lässt Sie einen Wiederherstellungspunkt im Sicherungs-Proxy-System einbinden. Um einen Wiederherstellungspunkt einzubinden, müssen Sie sich bei der CA ARCserve D2D-Benutzeroberfläche anmelden.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA ARCserve Central Protection Manager an, und klicken Sie in der Navigationsleiste auf "Knoten".
2. Blenden Sie im Fenster "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen möchten.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen möchten, und klicken Sie dann auf der Symbolleiste auf "Wiederherstellen".

   Eine CA ARCserve Central Host-Based VM Backup-Version von CA ARCserve D2D wird geöffnet.

   Hinweis: Stellen Sie sicher, dass die Pop-up-Optionen für Ihren Browser "alle Pop-up-Fenster" oder "Por-up-Fenster nur für diese Website" erlauben, sodass sich eine neue Browserinstanz öffnen kann.

Klicken Sie für weitere Details über den Dialog "Wiederherstellungspunkt laden" im Dialog auf der CA ARCserve D2D-Startseite auf "Hilfe".

Wiederherstellen von Daten mithilfe von "Wiederherzustellende Dateien/Ordner suchen"

Bei jeder erfolgreichen Sicherung durch die Anwendung werden alle gesicherten Dateien oder Ordner zum Snapshot-Image der Sicherung hinzugefügt. Mit dieser Wiederherstellungsmethode können Sie genau festlegen, welche Dateien oder Ordner wiederhergestellt werden sollen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

   Blenden Sie über die Ansicht "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen wollen.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen wollen, und danach in der Symbolleiste auf "Wiederherstellen".
2. Klicken Sie im Dialogfeld "Wiederherstellen" auf "Wiederherzustellende Dateien/Ordner suchen".

3. Geben Sie im Dialogfeld "Wiederherzustellende Dateien/Ordner suchen" den Speicherort der Sicherung an. Wenn Sie eine CA ARCserve Central Host-Based VM Backup-Sitzung wiederherstellen möchten, können Sie keinen Speicherort der Dateikopie angeben. Die Wiederherstellung der Dateikopie wird nur zugelassen, wenn Sie Sicherungssitzungen aus CA ARCserve Central Protection Manager oder CA ARCserve D2D wiederherstellen.

4. Geben Sie den Namen der Datei oder des Ordners, der wiederhergestellt werden soll, an.

   Hinweis: Das Feld "Dateiname" unterstützt die Suche nach vollständigen Namen oder mit Platzhaltern. Wenn Ihnen der vollständige Dateiname nicht bekannt ist, können Sie die Abfrage vereinfachen, indem Sie die Platzhalter "*" und "?" im Feld "Dateiname" eingeben.

   Folgende Platzhalter für den Datei- oder Ordnernamen werden unterstützt:

   - "*": Verwenden Sie den Asterisk, um null oder mehr Zeichen in einem Datei- oder Ordnernamen zu ersetzen.
   - "?": Verwenden Sie das Fragezeichen, um ein einzelnes Zeichen in einem Datei- oder Ordnernamen zu ersetzen.

   Beispiel: Wenn Sie *.txt angeben, werden alle Dateien mit einer .txt-Dateierweiterung in den Suchergebnissen angezeigt.

5. (Optional) Geben Sie einen Pfadnamen an, um Ihre Suche noch weiter zu filtern und wählen Sie aus, ob Unterverzeichnisse, Dateien und Ordner in der Suche berücksichtigt werden.

6. Klicken Sie auf "Suchen", um die Suche zu starten.

   Die Suchergebnisse werden angezeigt. Wenn mehrere Wiederherstellungspunkte für dieselbe Datei gefunden werden, werden alle Wiederherstellungspunkte nach Datum geordnet aufgelistet (der aktuellste steht an erster Stelle).

7. Wählen Sie aus der Liste die wiederherzustellende Version aus, und klicken Sie auf "Weiter".

   Das Dialogfeld "Optionen wiederherstellen" wird geöffnet. Sie können nur auf einem alternativen Speicherort wiederherstellen. Geben Sie den Pfad an oder durchsuchen Sie das System, um den Speicherort für das Sicherungs-Image auszuwählen. Klicken Sie auf den grünen Pfeil, um Verbindungen zu überprüfen. Geben Sie im Bedarfsfall die Benutzeranmeldeinformationen an.

8. Wählen Sie die Optionen zur Konfliktlösung aus:

   Vorhandene Dateien überschreiben

   Überschreibt (ersetzt) alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind. Alle Objekte werden aus den Sicherungsdateien wiederhergestellt, ohne Rücksicht darauf, ob sie auf Ihrem Rechner vorhanden sind.

   Aktive Dateien ersetzen

   Ersetzt alle aktiven Dateien nach einem Neustart. Wenn die Software während eines Wiederherstellungsversuchs erkennt, dass die vorhandene Datei gerade verwendet wird oder gerade auf sie zugegriffen wird, wird diese Datei nicht sofort ersetzt. Um Problemen vorzubeugen, wird das Ersetzen der aktiven Dateien auf den nächsten Neustart verschoben. (Die Wiederherstellung wird umgehend durchgeführt, aber das Ersetzen von aktiven Dateien findet beim nächsten Neustart statt).

   Hinweis: Wenn diese Option nicht ausgewählt ist, werden aktive Dateien bei der Wiederherstellung übersprungen.

   Dateien umbenennen

   Erstellt eine neue Datei, wenn der Dateiname vorhanden ist. Mit dieser Option wird die Quelldatei mit dem gleichen Namen kopiert, sie erhält jedoch am Ziel eine andere Erweiterung. Die Daten sind dann in einer neuen Datei wiederhergestellt.

   Vorhandene Dateien überspringen

   Überspringt alle vorhandenen Dateien, die am Wiederherstellungsziel gespeichert sind und überschreibt (ersetzt) sie nicht. Es werden nur Objekte aus den Sicherungsdateien wiederhergestellt, die derzeit nicht auf Ihrem Rechner vorhanden sind.

   Standardmäßig ist diese Option aktiviert.

9. (Optional) Wählen Sie "Stammverzeichnis erstellen" aus der Verzeichnisstruktur.

   Mit dieser Option wird die gleiche Stammverzeichnisstruktur im Wiederherstellungspfad erstellt.

   Hinweis: Wenn diese Option nicht ausgewählt wird, wird die Datei oder der Ordner direkt im Zielordner wiederhergestellt.

10. Geben Sie das Verschlüsselungskennwort der Sicherung ein, um die verschlüsselten Daten wiederherzustellen. Klicken Sie anschließend auf "Weiter".

    Das Dialogfeld "Wiederherstellungs-Übersicht" wird angezeigt.

11. Überprüfen Sie die angezeigten Informationen, um sicherzustellen, dass sämtliche Wiederherstellungsoptionen und Einstellungen korrekt sind.

    - Wenn die Zusammenfassung nicht korrekt ist, klicken Sie auf "Vorherige" und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.
    - Wenn die zusammenfassenden Informationen korrekt sind, klicken Sie auf "Fertig stellen", um den Wiederherstellungsprozess zu starten.

Wiederherstellen eines gesamten virtuellen Rechners

Sie können einen kompletten virtuellen Rechner aus einer CA ARCserve Central Host-Based VM Backup-Sitzung wiederherstellen.

Diese Sicherungsmethode ist der BMR-Methode ähnlich. Mit dieser Methode können Sie das Windows-Gastbetriebssystem, Anwendungen und Daten wiederherstellen.

Gehen Sie wie folgt vor:

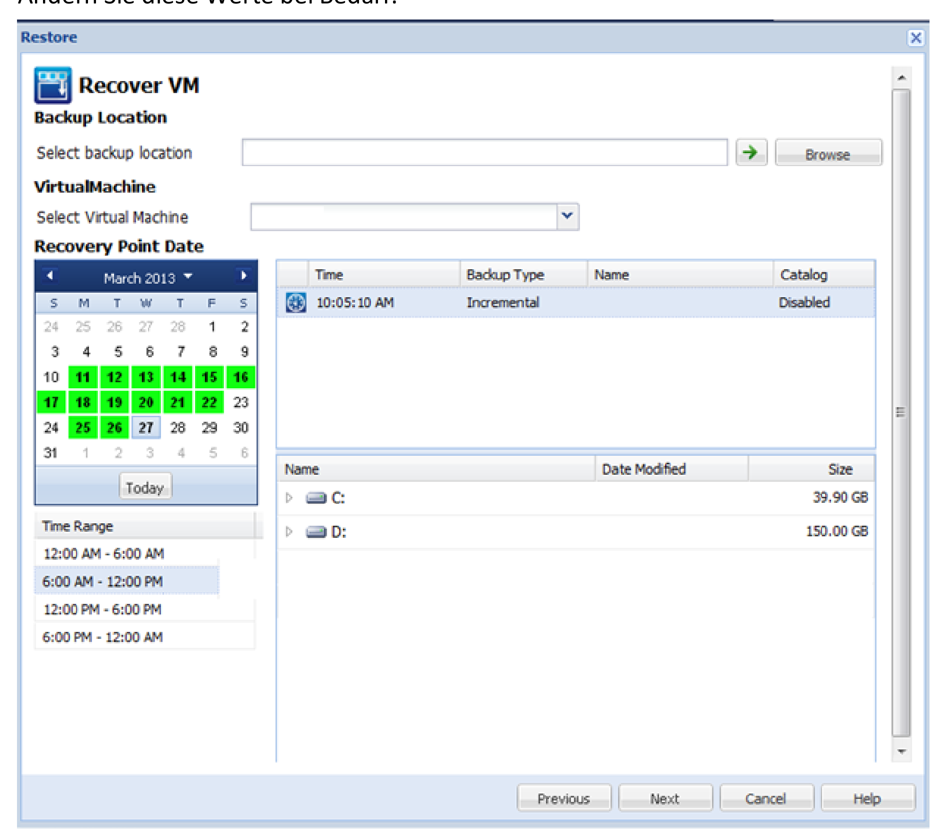
1. Melden Sie sich bei der Anwendung an und klicken Sie in der Navigationsleiste auf "Knoten".

   Blenden Sie im Fenster "Knoten" die Gruppe ein, die den Knoten enthält, den Sie wiederherstellen möchten.

   Klicken Sie auf das Kontrollkästchen neben dem Knoten, den Sie wiederherstellen möchten, und klicken Sie dann auf der Symbolleiste auf "Wiederherstellen". Die Anwendung meldet Sie an bei CA ARCserve D2D.

2. Klicken Sie im Dialogfeld "Wiederherstellen" auf "VM wiederherstellen".

3. Das Dialogfeld "Wiederherstellen" wird geöffnet. Die Felder "Speicherort für die Sicherung" und "Virtueller Rechner" wurden bereits aufgefüllt. Die angegebenen Daten hängen von der VM ab, die Sie im Fenster "Knoten" ausgewählt haben. Ändern Sie diese Werte bei Bedarf.



Geben Sie die Quelle an, wo Ihre Sicherungssitzungen virtueller Rechner gespeichert sind. Geben Sie Benutzeranmeldeinformationen ein, wenn Sie dazu aufgefordert werden.

In einem Drop-down-Menü werden alle virtuellen Rechner am Speicherort im Feld "Speicherort für die Sicherung" aufgelistet.

4. Klicken Sie im Kalender auf das Datum, für das Sie das Image des virtuellen Rechners wiederherstellen möchten. Klicken Sie in der Liste "Zeitraum" auf das wiederherzustellende Sicherungs-Image. Der Inhalt, der Ihrer Auswahl entspricht, wird zur Referenz angezeigt. Sie können keine einzelnen Volumes, Ordner oder Dateien auswählen. Der komplette virtuelle Rechner wird wiederhergestellt.

5. Klicken Sie auf "Weiter". Geben Sie im Dialogfeld "Wiederherstellungsoptionen" das Wiederherstellungsziel an.

   Am ursprünglichen Speicherort wiederherstellen

   Stellt den virtuellen Rechner am selben Speicherort wieder her, an dem das Sicherungs-Image erstellt wurde. Standardmäßig ist diese Option aktiviert.

   Weitere Informationen finden Sie im Abschnitt Wiederherstellung der VM am ursprünglichen Speicherort (siehe Seite 110).

   An einem alternativen Speicherort wiederherstellen

   Stellt den virtuellen Rechner an einem anderen Speicherort wieder her, an dem das Sicherungs-Image erstellt wurde.

   Weitere Informationen finden Sie im Abschnitt Wiederherstellung der VM an einem alternativen Speicherort (siehe Seite 112).

6. Aktivieren Sie die Optionen "Konfliktlösung" und "Nach der Wiederherstellung". Standardmäßig sind diese Optionen nicht aktiviert.

   - Bestehenden virtuellen Rechner überschreiben: Ersetzt sämtliche vorhandenen Images virtueller Rechner auf dem vCenter/ESX-Server.
   - Virtuellen Rechner starten: Der virtuelle Rechner wird nach Abschluss des Wiederherstellungsprozesses gestartet.

7. Klicken Sie auf "Weiter". Geben Sie die Anmeldeinformationen des vCenter-/ESX-Servers für die Sicherungsquelle an, wenn Sie dazu aufgefordert werden, und klicken Sie auf "OK".

8. Überprüfen Sie im Dialogfeld "Wiederherstellungs-Übersicht", ob alle Optionen korrekt angegeben wurden. Wenn nicht alle Einstellungen richtig sind, klicken Sie auf "Zurück". Wenn alle Einstellungen richtig sind, klicken Sie auf "Fertig stellen", um den Wiederherstellungsvorgang zu starten.

Wiederherstellen von virtuellen Rechnern an ursprünglichen Speicherorten

Während des Konfigurationsvorgangs zur Wiederherstellung der VM ist es erforderlich, dass Sie die Option auswählen, mit der Sie bestimmen können, wo der virtuelle Rechner wiederhergestellt wird. Die verfügbare Auswahl ist "Wiederherstellung am ursprünglichen Speicherort" und "Wiederherstellung an einem alternativen Speicherort".

Wenn Sie Ihre VM am ursprünglichen Speicherort wiederherstellen, führen Sie folgende Schritte aus:

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld "Wiederherstellungsoptionen", nachdem Sie die Optionen "Konflikte lösen" und "Nach der Wiederherstellung" angegeben haben, die Option "Am ursprünglichen Speicherort wiederherstellen" und klicken Sie auf "Weiter".

   Hinweis: Weitere Informationen über die Optionen "Konflikte lösen" und "Nach der Wiederherstellung" finden Sie im Abschnitt Wiederherstellen von Daten aus virtuellen Rechnern.

   Das Dialogfeld "Anmeldeinformationen für Quell-vCenter/ESX Server festlegen" wird angezeigt.

2. Geben Sie die Anmeldeinformationen ein, um auf den virtuellen Rechner zuzugreifen.

   - **vCenter/ESX Server**: Geben Sie den Hostnamen oder die IP-Adresse für das Ziel des vCenter- oder ESX-Serversystems an.
   - **VM-Name:** Legen Sie den Hostnamen des virtuellen Rechners fest, den Sie wiederherstellen.
   - **Protokoll:** Geben Sie das Protokoll an, das Sie für die Kommunikation mit dem Zielserver verwenden möchten. Die verfügbare Auswahl ist "HTTP" und "HTTPS".
   - **Portnummer:** Legen Sie den Port fest, den Sie für die Kommunikation zwischen dem Quellserver und dem Ziel verwenden möchten. Standardmäßig wird die Portnummer 443 angegeben.
   - **Benutzername:** Legen Sie den Benutzernamen fest, der über Zugriffsrechte zur Anmeldung am virtuellen Rechner, den Sie wiederherstellen, verfügt.
   - **Kennwort:** Geben Sie das entsprechende Kennwort für den Benutzernamen an, der für die Anmeldung am virtuellen Rechner, der wiederhergestellt wird, erforderlich ist.

3. Wenn alle Anmeldeinformationen angegeben sind, klicken Sie auf "OK".

   Das Dialogfeld "Wiederherstellungs-Übersicht" wird geöffnet.

4. Überprüfen Sie die angezeigten Informationen, um sicherzustellen, dass sämtliche Wiederherstellungsoptionen und Einstellungen korrekt sind.

   - Wenn die Zusammenfassung nicht korrekt ist, klicken Sie auf "Vorherige" und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.
   - Wenn die zusammenfassenden Informationen korrekt sind, klicken Sie auf "Fertig stellen", um den Wiederherstellungsprozess zu starten.

Wiederherstellen von virtuellen Rechnern an alternativen Speicherorten

Während des Konfigurationsvorgangs zur Wiederherstellung der VM ist es erforderlich, dass Sie die Option auswählen, mit der Sie bestimmen können, wo der virtuelle Rechner wiederhergestellt wird. Die verfügbare Auswahl ist "Wiederherstellung am ursprünglichen Speicherort" und "Wiederherstellung an einem alternativen Speicherort".

Wenn Sie den virtuellen Rechner an einem alternativen Speicherort wiederherstellen wollen, führen Sie folgende Schritte aus:

Gehen Sie wie folgt vor:

1. Wählen Sie im Dialogfeld "Wiederherstellungsoptionen", nachdem Sie die Optionen "Konflikte lösen" und "Nach der Wiederherstellung" angegeben haben, die Option "An einem alternativen Speicherort wiederherstellen".

   Hinweis: Weitere Informationen über die Optionen "Konflikte lösen" und "Nach der Wiederherstellung" finden Sie im Abschnitt Wiederherstellen von Daten auf virtuellen Rechnern.

   Das Dialogfeld "Wiederherstellungsoptionen" wird eingeblendet, um zusätzliche Optionen für Wiederherstellungen an alternativen Speicherorten anzuzeigen.

2. Geben Sie vCenter/ESX Server-Informationen an.

   - **vCenter/ESX Server**: Geben Sie den Hostnamen oder die IP-Adresse für das Ziel des vCenter- oder ESX-Serversystems an.
   - **Benutzername**: Legen Sie den Benutzernamen fest, der über Zugriffsrechte zur Anmeldung am virtuellen Rechner, den Sie wiederherstellen, verfügt.
   - **Kennwort:** Geben Sie das entsprechende Kennwort für den Benutzernamen an, der für die Anmeldung am virtuellen Rechner, der wiederhergestellt wird, erforderlich ist.
   - **Protokoll:** Geben Sie das Protokoll an, das Sie für die Kommunikation mit dem Zielserver verwenden möchten. Die verfügbare Auswahl ist "HTTP" und "HTTPS".
   - **Portnummer:** Legen Sie den Port fest, den Sie für die Kommunikation zwischen dem Quellserver und dem Ziel verwenden möchten. Standardmäßig wird die Portnummer 44 angegeben.

3. Wenn die vCenter/ESX Server-Informationen angegeben sind, klicken Sie auf die Schaltfläche "Stellen Sie eine Verbindung zum vCenter/ESX Server her".

   Wenn die alternativen Anmeldeinformationen für den Serverzugriff korrekt sind, werden die Felder "Weitere Informationen" aktiviert.

4. Geben Sie weitere Informationen an.

   - **VM-Name:** Legen Sie den Hostnamen des virtuellen Rechners fest, den Sie wiederherstellen.
   - **ESX Server:** Legen Sie den Ziel-ESX-Server fest. Das Drop-down-Menü enthält eine Auflistung aller ESX-Server, die mit dem angegebenen virtuellen Rechner verbunden sind.
   - **Ressourcenpool:** Legen Sie den Ressourcenpool oder vApp-Pool fest, den Sie für die VM-Wiederherstellung verwenden möchten. Klicken Sie auf die Schaltfläche "Ressourcenpool durchsuchen", um das Dialogfeld "Ressourcenpool auswählen" anzuzeigen. Dieses Dialogfeld enthält eine Auflistung aller verfügbaren Ressourcenpools und vApp-Pools für den Ziel-ESX-Server . Wählen Sie den Pool aus, der für die Wiederherstellung des virtuellen Rechners verwendet werden soll. Sie können dieses Feld leer lassen, wenn Sie dieser Wiederherstellung des Rechners keinen Ressourcenpool oder vApp-Pool zuweisen möchten.

     Hinweis: Ein Ressourcenpool ist eine konfigurierte Sammlung von CPU- und Speicherressourcen. Ein vApp-Pool ist eine Sammlung von einem oder mehreren virtuellen Rechnern, die als ein einzelnes Objekt verwaltet werden können.

   - **VM-Datenspeicher:**Geben Sie das Ziel des VM-Datenspeichers für die Wiederherstellung des virtuellen Rechners an, oder geben Sie jeden virtuellen Datenträger innerhalb des virtuellen Rechners an.

     Ein virtueller Rechner kann mehrere virtuelle Datenträger haben, und Sie können einen anderen Datenspeicher für jeden virtuellen Datenträger angeben.

     Beispiel:

     - Disk0 kann auf Datastore1 wiederhergestellt werden.
     - Disk1 kann auf Datastore1 wiederhergestellt werden.
     - Disk2 kann auf Datastore2 wiederhergestellt werden.

     Wichtig! Für VM-Datastore wird dieses Feld nur aufgefüllt, wenn der Benutzer vollständige Administratorrechte für das VMware-System hat. Wenn der Benutzer nicht über die entsprechenden Administratorrechte verfügt, wird CA ARCserve Central Host-Based VM Backup nicht mit dem Wiederherstellungsprozess fortfahren, nachdem Sie eine Verbindung zum vCenter/ESX-Server hergestellt haben.

5. Wenn "Weitere Informationen" angegeben sind, klicken Sie auf "Weiter".

   Das Dialogfeld "Wiederherstellungs-Übersicht" wird geöffnet.

6. Überprüfen Sie die angezeigten Informationen, um sicherzustellen, dass sämtliche Wiederherstellungsoptionen und Einstellungen korrekt sind.
   - Wenn die Zusammenfassung nicht korrekt ist, klicken Sie auf "Vorherige" und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.
   - Wenn die zusammenfassenden Informationen korrekt sind, klicken Sie auf "Fertig stellen", um den Wiederherstellungsprozess zu starten.

Hinweise zur Wiederherstellung

Verwenden Sie folgende Tabelle, um zu bestimmen, welche Wiederherstellungsmethode unter den aufgelisteten Bedingungen verwendet werden soll.

Wiederherstellungsmethode:	**Sie möchten:**	**Besondere Aspekte:**
Wiederherstellungspunkte durchsuchen (Verwenden Sie diese Methode zur Wiederherstellung auf Anwendungsebene.) Wiederherzustellende Dateien/Ordner suchen	Korrupte Dateien, Ordner, Datenbanken oder Anwendungen wiederherstellen	■ **CA ARCserve Central Host-Based VM Backup**: Zur Wiederherstellung von Dateien oder Ordnern muss der virtuelle Rechner zum Zeitpunkt der Sicherung eingeschaltet sein. Die Option "Am ursprünglichen Speicherort wiederherstellen" ist nicht verfügbar. Ordnen Sie ein Netzlaufwerk zum ursprünglichen Speicherort zu oder greifen Sie als Freigabe darauf zu. Führen Sie dann eine Wiederherstellung an dem zugeordneten oder freigegebenen Speicherort durch. Installieren Sie CA ARCserve D2D im Gast-BS eines neuen virtuellen Rechners, und stellen Sie eine Anwendungsdatenbank wieder her. Weitere Informationen finden Sie im Abschnitt "Wiederherstellungen auf Anwendungsebene". ■ **CA ARCserve D2D oder CA ARCserve Central Protection Manager**: Weitere Details finden Sie im Benutzerhandbuch.
VM wiederherstellen	Einen virtuellen Rechner bereitstellen und das Betriebssystem, die Anwendungen und Daten wiederherstellen	■ **CA ARCserve Central Host-Based VM Backup**: Empfohlen ■ **CA ARCserve D2D oder CA ARCserve Central Protection Manager**: Nicht Unterstützt

Die Wiederherstellung kann auch über BMR und auf Anwendungsebene durchgeführt werden. Weitere Informationen finden Sie im Thema Wiederherstellungsmethoden (siehe Seite 100).

Wiederherstellungen auf Anwendungsebene

CA ARCserve Central Applications ermöglicht es Ihnen, Daten zu schützen und wiederherzustellen. Sie können dabei auch Anwendungen, die diese Daten verwenden, sichern und ausführen. Die Wiederherstellung auf Anwendungsebene verwendet die Wiederherstellungsmethode "Wiederherstellungspunkte durchsuchen". Während der Wiederherstellung auf Anwendungsebene können Sie Microsoft Exchange Server oder SQL Server wiederherstellen, ohne eine vollständige Disaster Recovery ausführen zu müssen.

Bevor Sie die Wiederherstellung auf Anwendungsebene starten, müssen Sie möglicherweise Folgendes ausführen:

- Bereitstellen eines neuen virtuellen Rechners mit einem Windows Gast-BS
- Installieren von CA ARCserve D2D im Gast-BS
- Für Vorgänge der Anwendungswiederherstellung von Exchange Server:
  - Stellen Sie sicher, dass das Konto Berechtigungen einer vollständigen Administratorrolle für Exchange Server 2003 bzw. einer Administratorrolle der Exchange-Organisation oder der Server-Administratorrolle für Exchange Server 2007/2010/2013 hat.
  - Wenn Sie Exchange Server 2007-Datenbanken auf Wiederherstellungsspeichergruppen wiederherstellen, sollten Sie die Wiederherstellungsspeichergruppen auf dem geschützten Server erstellen. Wenn Sie Exchange Server 2010- oder 2013-Datenbanken in Wiederherstellungsdatenbanken wiederherstellen, erstellen Sie die Wiederherstellungsdatenbanken auf dem geschützten Server.
  - Sehen Sie sich noch einmal das komplette Verfahren zur Durchführung einer Wiederherstellung an, so wie im CA ARCserve D2D-Benutzerhandbuch dargestellt.

Wiederherstellen von Exchange Server-Daten

Sie können Wiederherstellungen auf Anwendungsebene von Microsoft Exchange Server-Daten mit Folgendem ausführen:

- Exchange Server 2003 - Einzelserverumgebung Die Cluster-Umgebung wird nicht unterstützt.
- Exchange Server 2007 - Einzelserverumgebung, Umgebung der fortlaufenden lokalen Replikation (LCR) und Umgebung der fortlaufenden Clusterreplikation (CCR) Installieren Sie für Exchange Server 2007 CCR CA ARCserve D2D lokal auf den aktiven und passiven Knoten. Sie können Sicherungsvorgänge entweder vom aktiven oder passiven Knoten ausführen, Wiederherstellungsvorgänge können jedoch nur auf dem aktiven Knoten ausgeführt werden. Einzelkopiecluster (SCC) wird nicht unterstützt.
- Exchange Server 2010: Einzelserverumgebung und Database Availability Group (DAG) Stellen Sie für eine DAG-Umgebung sicher, dass CA ARCserve D2D auf allen Servern in der DAG installiert ist. Sicherungen können auf allen Servern für aktive und passive Datenbankkopien durchgeführt werden, Wiederherstellungen können jedoch nur auf aktiven Datenbankkopien erfolgreich abgeschlossen werden.
- Microsoft Exchange 2013: Sicherung und Wiederherstellung von Microsoft Volumenschattenkopie-Dienst (VSS) wird unterstützt. Granular Recovery Technology (GRT) wird nicht unterstützt.

Sie können Microsoft Exchange Server-Daten auf den folgenden Ebenen wiederherstellen:

- Microsoft Exchange Writer-Ebene: Alle Exchange Server-Daten werden wiederhergestellt.
- Speichergruppenebene: Bestimmte Speichergruppe wird wiederhergestellt (gilt nicht für Microsoft Exchange Server 2010).
- Postfachspeicherebene: Bestimmter Postfachspeicher wird wiederhergestellt (gilt nur für Microsoft Exchange Server 2003).
- Postfachdatenbankebene: Bestimmte Postfachdatenbank wird wiederhergestellt (gilt für Exchange Server 2007 und 2010).

Hinweis: Bevor Sie beginnen, sollten Sie die notwendigen Voraussetzungen in Wiederherstellungen auf Anwendungsebene (siehe Seite 115) erfüllen.

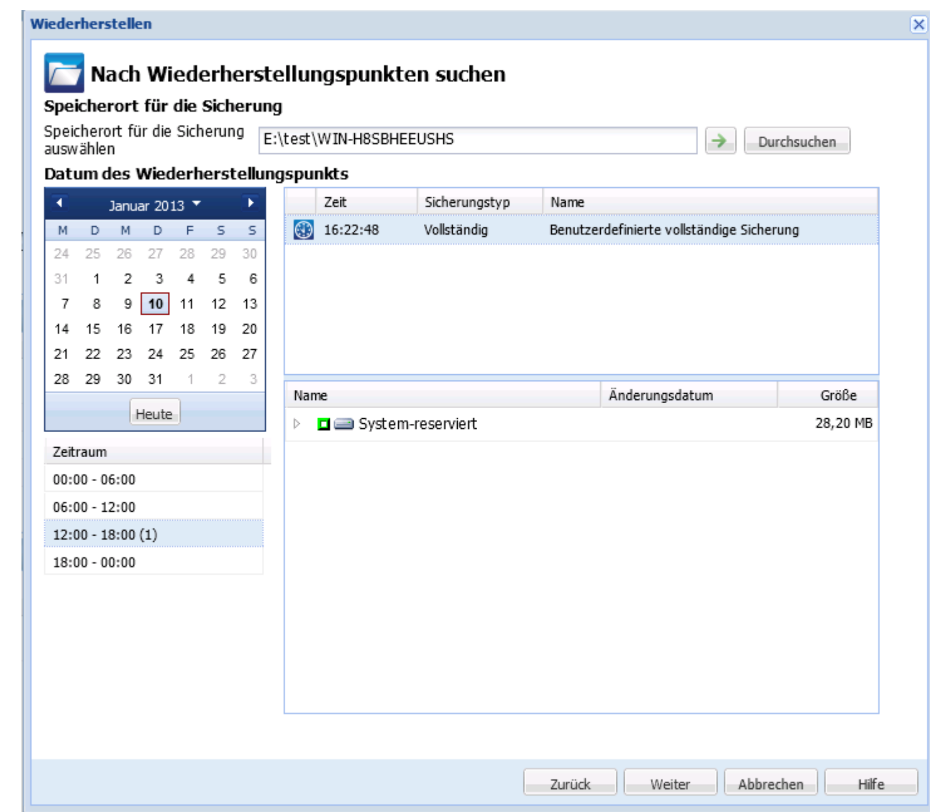
Wichtig! Die Wiederherstellung von Microsoft Exchange Server-Benutzerpostfachelementen wird von den CA ARCserve Central Host-Based VM Backup-Sitzungen nicht unterstützt. Um Microsoft Exchange Server-Daten auf spezifischer Ebene wiederherzustellen, sichern Sie die Exchange Server -Daten mithilfe von CA ARCserve Central Protection Manager oder CA ARCserve D2D.

So stellen Sie Exchange Server-Daten wieder her

1. Stellen Sie sicher, dass CA ARCserve D2D auf dem Gastbetriebssystem installiert ist.
2. Melden Sie sich beim Gastbetriebssystem auf dem virtuellen Rechner an, auf dem Sie Exchange Server-Daten wiederherstellen wollen.
3. Starten Sie CA ARCserve D2D und klicken Sie im Feld "Navigation" von CA ARCserve D2D auf "Wiederherstellen", um das Dialogfeld "Wiederherstellung" zu öffnen.
4. Klicken Sie auf das Dialogfeld "Wiederherstellungspunkte durchsuchen", um das Dialogfeld zum Durchsuchen der Wiederherstellungspunkte zu öffnen.
5. Legen Sie im Feld "Speicherort für die Sicherung auswählen" des Dialogfelds "Nach Wiederherstellungspunkten suchen" den Pfad zur Sicherungssitzung auf dem virtuellen Host-Based VM Backup-Rechner fest, von dem Sie Exchange Server-Daten sichern wollen. Der folgende Pfad ist ein Beispiel für den Pfad zur Sicherungssitzung auf dem virtuellen Host-Based VM Backup-Rechner:

   ```
   https://<Servername>/<Freigabename>/vm@<Hostname oder IP-Adresse des ESX
   Server-Systems>
   ```

6. Klicken Sie im Kalender auf ein Datum und die Uhrzeit der Wiederherstellung.



7. Klicken Sie auf "Weiter", um das Dialogfeld "Wiederherstellungsoptionen" zu öffnen.

8. Wählen Sie das Ziel für die Wiederherstellung aus.

   Es stehen Optionen zur Wiederherstellung am ursprünglichen Speicherort der Sicherheitskopie, zur ausschließlichen Wiederherstellung der Speicherauszugsdatei oder zur Wiederherstellung in einer Wiederherstellungsspeichergruppe/Wiederherstellungspostfachdatenbank zur Verfügung.

   Am ursprünglichen Speicherort wiederherstellen

   Stellt die Daten am selben Speicherort wieder her, von dem das Sicherungs-Image erstellt wurde.

Nur Speicherauszugsdatei

Stellt nur die Speicherauszugsdatei wieder her.

Mit dieser Option stellt CA ARCserve D2D die Microsoft Exchange-Datenbankdatei in einem festgelegten Ordner wieder her und stellt Sie nach der Wiederherstellung nicht online. Sie können diese Datei auf einen anderen Server verschieben und manuell in einem Exchange-Server laden, um die in der Datei enthaltenen Daten anzuzeigen.

Hinweis: Wenn eine Wiederherstellungspostfachdatenbank vorhanden ist, schlägt die Option "Nur Speicherauszugsdatei" fehl.

Protokoll in Datenbank wiedergeben

Legt fest, dass Sie alle Microsoft Exchange-Transaktionsprotokolldateien wiedergeben, anwenden und in die Datenbank übergeben können, wenn die Datenbankdateien im Zielordner gespeichert sind. Beim nächsten Start der Datenbank werden noch nicht eingetragene Transaktionsprotokolldateien angewendet, bevor Sie erneut Zugriff auf die Datenbank erhalten.

Hinweis: Diese Option ist nicht für Microsoft Exchange Server 2003 anwendbar.

In der Wiederherstellungsspeichergruppe wiederherstellen (Exchange 2007)

Stellt die Datenbank in einer Wiederherstellungsspeichergruppe (RSG) wieder her.

Eine RSG (Recovery Storage Group) ist eine Speichergruppe, die zu Wiederherstellungszwecken verwendet werden kann. Sie können eine gesicherte Microsoft Exchange-Postfachdatenbank in einer Wiederherstellungsspeichergruppe wiederherstellen und aus ihr Daten wiederherstellen und extrahieren, ohne, dass sich dies auf die Datenbank auswirkt, auf die von den Endbenutzern zugegriffen wird.

- Wenn eine einzelne Speichergruppe oder Datenbank (Öffentliche Ordner-Datenbank ausgenommen) aus derselben Speichergruppe zur Wiederherstellung ausgewählt wird, ist das standardmäßige Wiederherstellungsziel "In der Wiederherstellungsspeichergruppe wiederherstellen" (oder "In Wiederherstellungsdatenbank wiederherstellen").
- Wenn mehrere Speichergruppen oder Datenbanken aus mehreren Speichergruppen zur Wiederherstellung ausgewählt werden, kann Exchange nur am ursprünglichen Speicherort oder mit der Option "Nur Speicherauszugsdatei" wiederhergestellt werden. Das standardmäßige Wiederherstellungsziel ist "Am ursprünglichen Speicherort wiederherstellen".

Bevor Sie eine Exchange 2007-Datenbank in einer Wiederherstellungsspeichergruppe wiederherstellen können, müssen Sie eine Wiederherstellungsspeichergruppe und eine Postfachdatenbank mit demselben Namen erstellen.

Wenn Sie zum Beispiel "Postfachdatenbank1" aus der ersten Speichergruppe in einer Wiederherstellungsspeichergruppe wiederherstellen möchten, müssen Sie eine Wiederherstellungsspeichergruppe erstellen und die Datenbank "Postfachdatenbank1" zur Wiederherstellungsspeichergruppe hinzufügen.

Hinweis: Diese Option ist nicht für Microsoft Exchange Server 2003 anwendbar.

Datenbank vor der Wiederherstellung entladen und sie nach der Wiederherstellung erneut laden

Normalerweise führt Microsoft Exchange vor einer Wiederherstellung einige Überprüfungen durch, um Folgendes sicherzustellen:

- Die Datenbank, die wiederhergestellt werden soll, hat den Status "Bereitstellung aufgehoben".
- Die Datenbank wird nicht unerwartet wiederhergestellt.

  Damit eine Microsoft Exchange-Produktionsdatenbank nicht unerwartet wiederhergestellt wird, wird ein Schalter hinzugefügt, sodass die Datenbank während der Wiederherstellung überschrieben werden kann. Microsoft Exchange wird keine Datenbanken wiederherstellen, wenn dieser Schalter nicht festgelegt ist.

Bei CA ARCserve D2D werden diese zwei Optionen über die Option "Datenbank vor der Wiederherstellung entladen und nach der Wiederherstellung erneut laden" gesteuert. Mit dieser Option können Sie die Wiederherstellung in CA ARCserve D2D automatisch, ohne manuelle Vorgänge, starten. (Sie können auch angeben, Datenbanken manuell zu entladen/laden)

- Wenn Sie diese Option markieren, wird die Exchange-Datenbank vor dem Wiederherstellungsprozess automatisch entladen, und nach Abschluss der Wiederherstellung erneut geladen. Wenn diese Option aktiviert ist, können Exchange-Datenbanken während der Wiederherstellung überschrieben werden.
- Wenn dieses Kästchen nicht markiert ist, wird die Exchange-Datenbank vor der Wiederherstellung nicht automatisch entladen und nach der Wiederherstellung nicht erneut geladen.

  Der Exchange-Administrator müsste dann einige manuelle Vorgänge ausführen, wie z. B. die Exchange-Datenbank entladen, die Markierung "Überschreibung zulassen" auf die Datenbank setzen und die Exchange-Datenbank laden. (Exchange führt den Wiederherstellungsvorgang während dem Laden der Datenbank aus)

  Wenn diese Option nicht aktiviert ist, können Exchange-Datenbanken während der Wiederherstellung nicht überschrieben werden.

In Wiederherstellungsdatenbank wiederherstellen (Exchange 2010)

Stellt die Datenbank in einer Wiederherstellungsdatenbank wieder her. Eine Wiederherstellungsdatenbank ist eine Datenbank, die für Wiederherstellungen verwendet werden kann. Sie können eine gesicherte Microsoft Exchange-Postfachdatenbank in einer Wiederherstellungsdatenbank wiederherstellen und aus ihr Daten wiederherstellen und extrahieren, ohne, dass sich dies auf die Datenbank auswirkt, auf die von den Endbenutzern zugegriffen wird.

Bevor Sie eine Wiederherstellung einer Exchange 2010-Datenbank in einer Wiederherstellungsdatenbank durchführen, müssen Sie zunächst eine Wiederherstellungsdatenbank erstellen.

Hinweis: Diese Option ist nicht für Microsoft Exchange Server 2003 und 2007 anwendbar.

9. Klicken Sie auf "Weiter", um das Dialogfeld "Wiederherstellungs-Übersicht" zu öffnen.
10. Überprüfen Sie die angezeigten Informationen, um sicherzustellen, dass sämtliche Wiederherstellungsoptionen und Einstellungen korrekt sind.
    - Wenn die Übersichtsinformationen nicht korrekt sind, klicken Sie auf Zurück, und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.
    - Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf Fertig stellen, um den Wiederherstellungsprozess zu starten.

Wiederherstellen von SQL Server-Daten

Sie können Wiederherstellungen auf Anwendungsebene von Microsoft SQL Server-Daten mit Folgendem ausführen:

- Microsoft SQL Server 2005 Express/Standard/Workgroup/Enterprise
- Microsoft SQL Server 2008, SQL Server 2008 R2 Express/Web/Standard/Workgroup/Enterprise

Hinweis: Bevor Sie mit den Vorgängen beginnen, lesen Sie die Voraussetzungen in Wiederherstellungen auf Anwendungsebene (siehe Seite 115).

Wichtig! Spezifische Wiederherstellung für Microsoft SQL Server funktioniert nicht auf der CA ARCserve Central Host-Based VM Backup-Konsole. Um Microsoft SQL Server-Daten wiederherzustellen, installieren Sie CA ARCserve D2D auf dem virtuellen Gastrechner.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass CA ARCserve D2D auf dem Gastbetriebssystem installiert ist.
2. Melden Sie sich beim Gastbetriebssystem für den virtuellen Rechner an, auf dem Sie SQL Server-Daten wiederherstellen wollen.

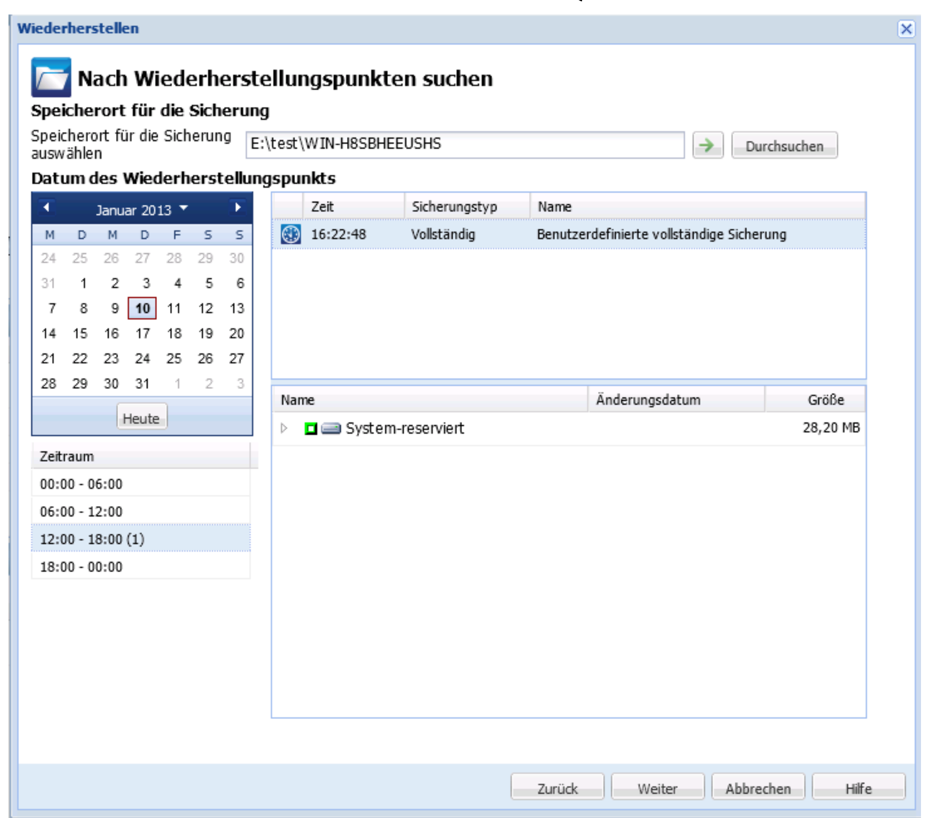
3. Starten Sie CA ARCserve D2D und klicken Sie im Feld "Navigation" von CA ARCserve D2D auf "Wiederherstellen", um das Dialogfeld "Wiederherstellung" zu öffnen.

4. Klicken Sie auf das Dialogfeld "Wiederherstellungspunkte durchsuchen", um das Dialogfeld zum Durchsuchen der Wiederherstellungspunkte zu öffnen.

5. Legen Sie im Feld "Speicherort für die Sicherung auswählen" des Dialogfelds "Nach Wiederherstellungspunkten suchen" den Pfad zur Sicherungssitzung auf dem virtuellen Host-Based VM Backup-Rechner fest, von dem Sie SQL Server-Daten sichern wollen. Der folgende Pfad ist ein Beispiel für den Pfad zur Sicherungssitzung auf dem virtuellen Host-Based VM Backup-Rechner:

```
https://<Servername>/<Freigabename>/vm@<Hostname oder IP-Adresse des ESX
Server-Systems>
```

6. Wählen Sie zunächst den Wiederherstellungspunkt (Datum und Uhrzeit), und anschließend die wiederherzustellende Microsoft SQL Server-Datenbank.



7. Klicken Sie auf "Weiter", um das Dialogfeld "Wiederherstellungsoptionen" zu öffnen.

   Wählen Sie das Ziel für die Wiederherstellung aus. Es stehen Optionen zur Wiederherstellung am ursprünglichen Speicherort, zur ausschließlichen Wiederherstellung der Speicherauszugsdatei oder zur Wiederherstellung an einem alternativen Speicherort zur Verfügung.

   Am ursprünglichen Speicherort wiederherstellen

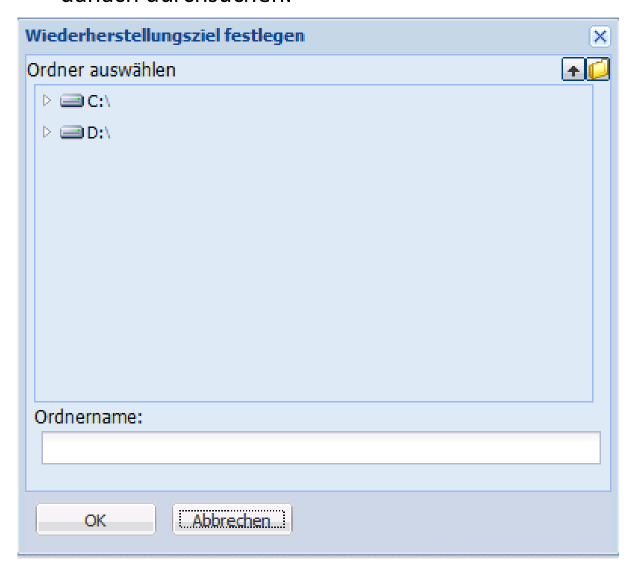
   Stellt die Daten am selben Speicherort wieder her, von dem das Sicherungs-Image erstellt wurde.

   Nur Speicherauszugsdatei

   Stellt nur die Speicherauszugsdatei wieder her.

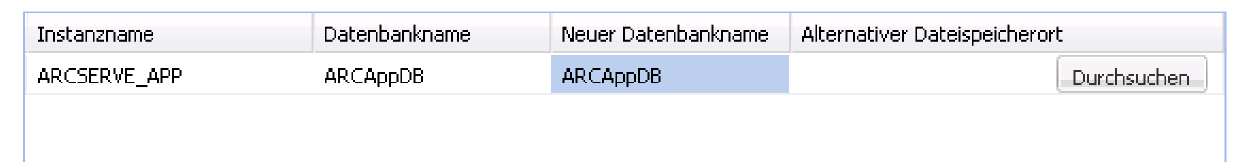
   Speicherauszugsdateien werden erstellt, wenn eine Anwendung abstürzt, die zusätzliche Informationen (mit Zeitstempel) enthält, die für die Fehlerbehebung verwendet werden können.

   Wenn diese Option ausgewählt ist, können Sie den Ordner, in dem die Speicherauszugsdatei wiederhergestellt wird, festlegen oder das System danach durchsuchen.

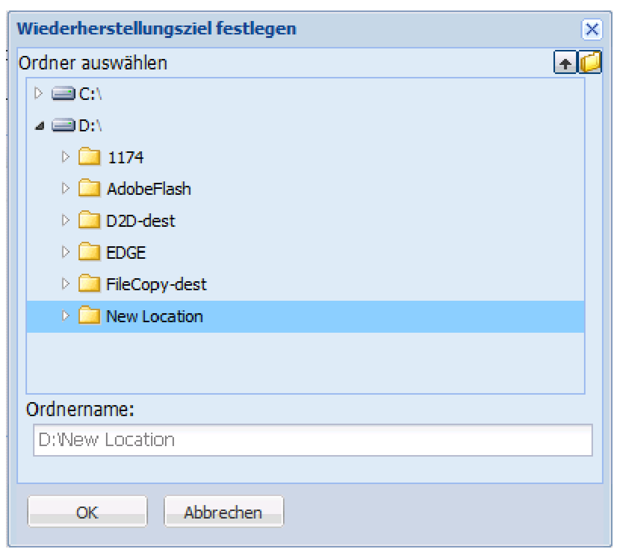


   An einem alternativen Speicherort wiederherstellen

   Stellt an einem alternativen Speicherort wieder her (nicht am ursprünglichen Speicherort).



Da Sicherungen in Netzwerkspeicherort kopiert werden können, können Sie von mehreren SQL Server-Instanzen verwendet werden. Ausgehend von der Instanzenebene können gleichzeitig mehrere Datenbanken wiederhergestellt werden. Sie können aus dieser Liste die Datenbankinstanz auswählen und einen neuen Datenbanknamen sowie einen alternativen Speicherort für ihre Wiederherstellung angeben. Zusätzlich können Sie das System nach dem alternativen Speicherort für die Wiederherstellung durchsuchen.



8. Klicken Sie auf "Weiter", um das Dialogfeld "Wiederherstellungs-Übersicht" zu öffnen.
9. Überprüfen Sie die angezeigten Informationen, um sicherzustellen, dass sämtliche Wiederherstellungsoptionen und Einstellungen korrekt sind.
   - Wenn die Übersichtsinformationen nicht korrekt sind, klicken Sie auf Zurück, und ändern Sie die falschen Einstellungen im entsprechenden Dialogfeld.
   - Wenn die Übersichtsinformationen korrekt sind, klicken Sie auf Fertig stellen, um den Wiederherstellungsprozess zu starten.

Kapitel 5: Fehlerbehebung in CA ARCserve Central Host-Based VM Backup

Dieser Abschnitt enthält Informationen zur Fehlerbehebung, mit deren Hilfe Sie Probleme erkennen und lösen können, die bei der Verwendung von CA ARCserve Central Host-Based VM Backup möglicherweise auftreten.

Dieses Kapitel enthält folgende Themen:

Beim Hinzufügen von Knoten zeigt eine Fehlermeldung an, dass keine Verbindung zum angegebenen Server möglich ist.

Gültig auf Windows-Plattformen.

Symptom:

Wenn Sie versuchen, Knoten über den Bildschirm "Knoten" hinzuzufügen oder zu verbinden, wird folgende Meldung angezeigt:

```
Es kann keine Verbindung zum festgelegten Server hergestellt werden.
```

Lösung:

Wenn die obige Meldung angezeigt wird, wenn Sie am Bildschirm "Knoten" Knoten hinzufügen möchten, können die folgenden korrigierenden Maßnahmen bei der Problemlösung helfen:

- Stellen Sie sicher, dass der Windows Server-Dienst auf dem CA ARCserve Central Host-Based VM Backup-Server und auf dem virtuellen Quellrechner (dem Knoten) ausgeführt wird.
- Stellen Sie sicher, dass auf den Datei- und Druckerfreigabedienst von Windows auf dem CA ARCserve Central Host-Based VM Backup-Server und auf dem virtuellen Quellrechner (dem Knoten) eine Windows-Firewallausnahme angewendet ist.
- Stellen Sie sicher, dass auf den Windows-Anmeldedienst nur dann eine Windows-Firewallausnahme angewendet ist, wenn der Knoten kein Mitglied einer Domäne ist. Führen Sie diesen Vorgang sowohl auf dem CA ARCserve Central Host-Based VM Backup-Server als auch auf dem virtuellen Quellrechner (dem Knoten) durch.

- Stellen Sie sicher, dass dem Modul "Freigabe und Sicherheit" des lokalen Kontos der Wert "Klassisch" zugeordnet ist. Gehen Sie wie folgt vor, um den Wert "Klassisch" anzuwenden:

  Hinweis: Führen Sie die folgenden Schritte sowohl auf dem CA ARCserve Central Host-Based VM Backup-Server als auch auf dem virtuellen Quellrechner (dem Knoten) durch.

  1. Melden Sie sich beim CA ARCserve Central Host-Based VM Backup-Server an, und öffnen Sie die Systemsteuerung.
  2. Öffnen Sie in der Systemsteuerung "Verwaltung".
  3. Doppelklicken Sie auf "Lokale Sicherheitsrichtlinie".

     Das Fenster "Lokale Sicherheitsrichtlinie" wird geöffnet.
  4. Erweitern Sie im Fenster "Lokale Sicherheitsrichtlinie" "Sicherheitsoptionen".

     Die Sicherheitsrichtlinien werden angezeigt.
  5. Klicken Sie mit der rechten Maustaste auf "Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten", und klicken Sie im Pop-up-Menü auf "Eigenschaften".

     Das Dialogfeld "Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten" wird geöffnet.
  6. Klicken Sie auf "Lokale Sicherheitseinstellung".

     Wählen Sie aus der Drop-down-Liste "Klassisch - lokale Benutzer authentifizieren sich als sie selbst" aus.

     Klicken Sie auf "OK".

- Stellen Sie sicher, dass der auf die lokalen Richtlinien für die LAN Manager-Authentifizierungsebene angewendete Wert festgelegt wird, um LM & NTLMv2 zu senden. Verwenden von NTLMv2-Sitzungssicherheit, wenn diese verhandelt wurde. Gehen Sie wie folgt vor, um den Wert anzuwenden:

  1. Melden Sie sich beim CA ARCserve Central Host-Based VM Backup-Server an, und öffnen Sie die Eingabeaufforderung.

     Führen Sie den folgenden Befehl aus:

     ```
     secpol.msc
     ```

     Das Dialogfeld "Lokale Sicherheitseinstellungen" wird geöffnet.
  2. Wählen Sie lokale Einstellungen aus, und klicken Sie auf die Sicherheitsoptionen.

     Suche nach Netzwerksicherheit: LAN Manager-Authentifizierungsebene.

     Doppelklicken Sie auf die Option.

     Das Dialogfeld "Eigenschaften" wird geöffnet.

3. Wählen Sie die entsprechende Option aus, und klicken Sie auf "OK".

   ```
   Senden Sie LM & NTLMv2 - Verwenden Sie NTLMv2-Sitzungssicherheit, wenn diese verhandelt wurde
   ```

4. Führen Sie in der Eingabeaufforderung folgenden Befehl aus:

   ```
   gpupdate
   ```

Der Wert wird angewendet.

Leere Webseiten oder JavaScript-Fehler treten auf

Gültig für Windows Server 2008- und Windows Server 2003-Betriebssysteme.

Symptom:

Wenn Sie CA ARCserve Central Applications-Websites in Internet Explorer öffnen, werden leere Webseiten angezeigt, oder es treten JavaScript-Fehler auf. Das Problem tritt auf, wenn Internet Explorer unter Windows Server 2008- und Windows Server 2003-Betriebssystemen geöffnet wird.

Dieses Problem tritt unter den folgenden Bedingungen auf:

- Sie verwenden Internet Explorer 8 oder Internet Explorer 9, um Ihre Anwendung anzuzeigen, und der Browser erkennt die URL nicht als vertrauenswürdige Seite an.
- Sie verwenden Internet Explorer 9, um Ihre Anwendung anzuzeigen, und verwenden dabei als Übertragungsprotokoll HTTPS.

Lösung:

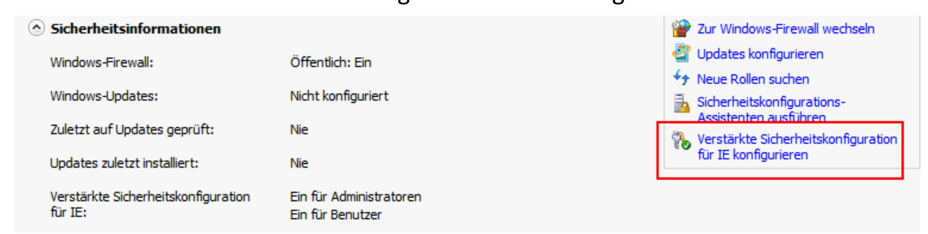
Um dieses Problem zu korrigieren, deaktivieren Sie auf den Computern, die Sie für die Anzeige der Anwendung verwenden möchten, die verstärkte Sicherheitskonfiguration für Internet Explorer.

Um die verstärkte Sicherheitskonfiguration für Internet Explorer unter Windows Server 2008-Systemen zu deaktivieren, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows Server 2008-Computer, den Sie für die Berichtsanzeige verwenden, über das Administratorkonto oder ein Konto mit administrativen Berechtigungen an.
2. Klicken Sie mit der rechten Maustaste auf dem Desktop auf "Computer", und klicken Sie anschließend auf "Verwalten", um das Fenster "Server-Manager " zu öffnen.

3. Klicken Sie im Fenster "Server-Manager " auf "Server-Manager (Servername)".

   Öffnen Sie "Sicherheitsinformationen" im Abschnitt "Serverübersicht", und klicken Sie auf "Verstärkte Sicherheitskonfiguration für IE konfigurieren":



   Das Dialogfeld "Verstärkte Sicherheitskonfiguration für Internet Explorer" wird geöffnet.

4. Gehen Sie im Dialogfeld "Verstärkte Sicherheitskonfiguration für Internet Explorer" folgendermaßen vor:

   - Deaktivieren Sie "Administratoren".
   - Deaktivieren Sie "Benutzer".

   Klicken Sie auf "OK".

Das Dialogfeld "Verstärkte Sicherheitskonfiguration für Internet Explorer" wird geschlossen, und die verstärkte Sicherheit Internet Explorer Sicherheit ist deaktiviert.

Um die verstärkte Sicherheitskonfiguration für Internet Explorer unter Windows Server 2003-Systemen zu deaktivieren, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows Server 2003-Computer, den Sie für die Berichtsanzeige verwenden, über das Administratorkonto oder ein Konto mit administrativen Berechtigungen an.
2. Öffnen Sie die Windows-Systemsteuerung, und öffnen Sie "Software".
3. Klicken Sie im Dialogfeld "Software" auf die Option für Windows-Komponenten "Hinzufügen/Entfernen", um auf den Assistenten für Windows-Komponenten zuzugreifen.

   Entfernen Sie dass das Häkchen neben "Verstärkte Sicherheitskonfiguration für Internet Explorer".

   Klicken Sie auf "Weiter".

   Folgen Sie den Anweisungen auf dem Bildschirm, um die Konfiguration abzuschließen, und klicken Sie auf "Fertig stellen".

Die verstärkte Sicherheit für Internet Explorer wird deaktiviert.

Bei Anmeldung in CA ARCserve D2D-Knoten laden sich Webseiten nicht richtig

Gültig auf Windows-Plattformen.

Symptom:

Webseiten in Browserfenstern laden sich nicht richtig, zeigen Fehlermeldungen an oder beides, wenn man sich vom Bildschirm "Knoten" aus bei CA ARCserve D2D-Knoten anmeldet.

Lösung:

Dieses Verhalten wirkt sich hauptsächlich auf Internet Explorer-Browser aus. Webseiten laden möglicherweise nicht richtig, wenn "Active scripting", ActiveX-Steuerelemente oder Java-Programme auf Ihrem Computer deaktiviert oder auf Ihrem Netzwerk gesperrt sind.

Sie können das Problem durch Aktualisieren Ihres Browserfensters beheben. Wenn das Aktualisieren Ihres Browserfensters das Problem jedoch nicht löst, gehen Sie wie folgt vor:

1. Öffnen Sie den Internet Explorer.

   Klicken Sie im Menü "Extras" auf "Internetoptionen".

   Das Dialogfeld "Internetoptionen" wird geöffnet.

2. Klicken Sie auf die Registerkarte "Sicherheit".

   Die Sicherheitsoptionen werden angezeigt.

3. Klicken Sie auf "Internetzone".

   Die Optionen der Internetzonen werden angezeigt.

4. Klicken Sie auf "Stufe anpassen".

   Das Dialogfeld "Sicherheitseinstellungen - Internetzone" öffnet sich.

5. Blättern Sie bis zur Kategorie "Scripting".

   Suchen Sie "Active Scripting".

   Klicken Sie auf die Option "Aktivieren" oder "Auffordern".

6. Klicken Sie in den Sicherheitseinstellungen auf das Dialogfeld "OK Internetzone".

   Das Dialogfeld "Sicherheitseinstellungen - Internetzone" wird geschlossen.

7. Klicken Sie im Dialogfeld "Internetoptionen" auf "OK".

   Das Dialogfeld "Internetoptionen" wird geschlossen und die Option "Active Scripting" wird angewendet.

Hinweis: Wenn diese Lösung das Problem nicht behebt, setzen Sie sich mit Ihrem Systemadministrator in Verbindung und stellen Sie sicher, dass andere Programme wie Antivirus- oder Firewall-Programme "Active Scripting", ActiveX-Steuerelemente oder Java-Programme nicht blockieren.

Beheben von Problemen beim Laden von Seiten

Gültig auf Windows-Plattformen.

Symptom:

Die folgenden Fehlermeldungen werden in Browserfenstern angezeigt, wenn Sie sich bei CA ARCserve Central Applications-, CA ARCserve D2D-Knoten und Überwachungsserver anmelden.

Meldung 1:

`Fehler auf dieser Webseite können zu Fehlern bei der Ausführung führen.`

Meldung 2:

`!`

Lösung:

Webseiten werden aus verschiedenen Gründen nicht richtig geladen. Die folgende Tabelle beschreibt häufige Gründe und die entsprechenden Korrekturmaßnahmen:

Ursache	Korrekturmaßnahme
Es gibt Probleme mit dem zugrunde liegenden HTML-Quellcode.	Aktualisieren Sie die Webseite und versuchen Sie es erneut.
Ihr Netzwerk blockiert "Active Scripting", ActiveX oder Java-Programme.	Lassen Sie zu, dass Ihr Browser "Aktive Scripting", ActiveX oder Java-Programme verwendet.
Ihre Antivirusanwendung ist so konfiguriert, dass temporäre Internetdateien und heruntergeladene Programme durchsucht werden.	Filtern Sie Ihre Antivirusanwendung so, dass mit CA ARCserve Central Applications-Webseiten in Zusammenhang stehende Dateien aus dem Internet zugelassen werden.

Ursache	Korrekturmaßnahme
Das auf Ihrem Computer installierte Skriptmodul ist fehlerhaft oder veraltet.	Aktualisieren Sie das Skriptmodul.
Die auf Ihrem Computer installierten Treiber für die Grafikkarte sind fehlerhaft oder veraltet.	Aktualisieren Sie die Treiber für die Grafikkarte.
Die auf Ihrem Computer installierte DirectX-Komponente ist fehlerhaft oder veraltet.	Aktualisieren Sie die DirectX-Komponente.

Störzeichen werden in Browser-Fenstern angezeigt, wenn man auf CA ARCserve Central Applications zugreift.

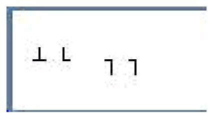
Gültig auf allen unterstützten Windows-Betriebssystemen. Gilt für alle Browser.

Symptom:

Wenn Sie sich bei CA ARCserve Central Applications anmelden, werden Störzeichen im Inhaltsbereich Ihres Browserfensters angezeigt.

Lösung:

Dieses Problem tritt auf, wenn Sie CA ARCserve Central Applications mithilfe von HTTPS-Kommunikation installieren und dann versuchen, auf CA ARCserve Central Applications mithilfe von HTTP-Kommunikation zuzugreifen. Die zugrunde liegende Webservices-Komponente in CA ARCserve Central Applications unterstützt den Wechsel von HTTP-URLs zu HTTPS-URLs nicht. Dadurch werden Störzeichen in Ihrem Browserfenster angezeigt. Beispiel:



Um dieses Problem zu beheben, greifen Sie mithilfe von HTTPS auf CA ARCserve Central Applications zu, wenn Sie die Anwendungen installieren oder konfigurieren, um mithilfe von HTTPS zu kommunizieren.

Zugriffsverweigerungsfehler beim Aktualisieren von Knoten

Gültig für alle Windows-Betriebssysteme, die Benutzerkontensteuerung (User Access Control, UAC) unterstützen.

Hinweis: Windows Vista oder höhere Versionen.

Symptom 1:

Wenn Sie ein Windows-Benutzerkonto angeben, das kein integriertes Administrator- oder Domänenbenutzerkonto, sondern Mitglied der Administratorgruppe ist, wird die folgende Meldung angezeigt, wenn das Kennwort im Dialogfeld "Knoten-Anmeldeinformationen" des Dialogfeld "Virtuelle Rechner aus vCenter/ESX importieren" angewandt wird:

```
Administratorrechte sind erforderlich.
```

Das Ergebnis ist, dass Sie die Knoten-Anmeldeinformationen nicht anwenden können.

Symptom 2:

Wenn Sie Knoten importieren, aber während des Importvorgangs keine Knoten-Anmeldeinformationen angeben, wird die folgende Meldung angezeigt, wenn Sie versuchen, den Vorgang "Knoten aktualisieren" mithilfe eines Windows-Benutzerkontos auszuführen, das kein integriertes Administrator- oder Domänenbenutzerkonto, sondern Mitglied der Administratorgruppe ist:

```
Zugriff verweigert. Stellen Sie sicher, dass der Benutzer Administratorrechte hat und der Remote-Registrierungszugriff nicht durch eine lokale Sicherheitsrichtlinie des hinzugefügten Rechners beschränkt ist.
```

Das Ergebnis ist, dass Sie den Knoten nicht aktualisieren können.

Lösung:

Dieses Verhalten ist zu erwarten, wenn UAC (User Account Control, Benutzerkontensteuerung) auf Computern aktiviert ist, auf denen ein Windows-Betriebssystem ausgeführt wird, das UAC unterstützt. UAC ist eine Windows-Funktion, durch die es ausschließlich dem Administratorkonto ermöglicht wird, sich von einem Remote-Standort an dem Computer anzumelden.

Verwenden Sie eine der folgenden Methoden, um dieses Problem zu lösen:

- Geben Sie die mitgelieferten Anmeldeinformationen oder die Anmeldeinformationen des Domänenadministrators an.
- Deaktivieren von UAC:
  1. Melden Sie sich über das Administratorkonto beim Knoten an.
  2. Öffnen Sie die Windows-Systemsteuerung.
  3. Öffnen Sie die Benutzerkonten.
  4. Klicken Sie im Fenster "Änderungen am eigenen Konto durchführen" auf "Einstellungen der Benutzerkontensteuerung ändern", und führen Sie anschließend einen der folgenden Schritte durch:
     - **Windows Vista und Windows Server 2008:** Klicken Sie im Fenster "Änderungen am eigenen Konto durchführen" auf "Benutzerkontensteuerung ein- oder ausschalten" Deaktivieren Sie anschließend im Fenster "Benutzerkontensteuerung einschalten, um den Computer sicherer zu machen" das Kontrollkästchen neben "Benutzerkontensteuerung verwenden, um zum Schutz des Computers beizutragen", und klicken Sie auf "OK".

       Starten Sie Ihren Computer neu, um die Änderungen auf UAC anzuwenden.
     - **Windows Server 2008 r2 und Windows 7:** Schieben Sie im Fenster "Benachrichtigungen über Änderungen an dem Computer auswählen" den Regler von "Immer benachrichtigen" auf "Nie benachrichtigen". Klicken Sie auf OK und schließen Sie die Windows-Systemsteuerung.

       Starten Sie Ihren Computer neu, um die Änderungen auf UAC anzuwenden.

Beim Anmeldung in der Anwendung wird ein Zertifikatsfehler angezeigt.

Gültig auf Windows-Plattformen.

Symptom:

Die folgende Meldung wird in Ihrem Browserfenster angezeigt, wenn Sie sich bei der Anwendung anmelden:

- Internet Explorer:

  `Es gibt ein Problem mit dem Sicherheitszertifikat dieser Website.`

- Firefox:

  `Diese Verbindung ist nicht vertrauenswürdig.`

- Chrome:

  `Dem Sicherheitszertifikat dieser Seite wird nicht vertraut!`

Wenn Sie eine Option angeben, mit der Sie zur Website gelangen, können Sie erfolgreich bei der Anwendung anmelden. Dieses Verhalten tritt jedoch jedes Mal auf, wenn Sie sich bei der Anwendung anmelden.

Lösung:

Dieses Verhalten tritt auf, wenn Sie angeben, dass HTTPS als Kommunikationsprotokoll verwendet werden soll. Um dieses Problem vorübergehend zu korrigieren, klicken Sie in Ihrem Browserfenster auf den Link, mit dem Sie weiter zur Website gelangen. Diese Meldung wird jedoch jedes Mal angezeigt werden, wenn Sie sich bei der Anwendung anmelden.

Das HTTPS-Kommunikationsprotokoll bietet eine höhere Sicherheitsebene als das HTTP-Kommunikationsprotokoll. Wenn Sie weiterhin unter Verwendung eines HTTPS-Kommunikationsprotokolls kommunizieren möchten, können Sie ein Sicherheitszertifikat von VeriSign erwerben und das Zertifikat auf dem Anwendungsserver installieren. Optional können Sie das von der Anwendung verwendete Kommunikationsprotokoll in HTTP ändern. Um das Kommunikationsprotokoll in HTTP zu ändern, gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Server an, auf dem Sie die Anwendung installiert haben.
2. Wechseln Sie zu dem folgenden Verzeichnis:

   `C:\Programme\CA\ARCserve Central Applications\BIN`
3. Führen Sie die folgende Batch-Datei aus:

   `ChangeToHttp.bat`
4. Nachdem die Batch-Datei ausgeführt wurde, öffnen Sie Windows Server Manager.

   Starten Sie den folgenden Dienst neu:

   `CA ARCserve Central Applications Service`

Sicherungen schlagen mit Snapshot-Erstellungsfehlern fehl

Gültig auf Windows-Plattformen.

Wenn Sie Sicherungen von VMware-basierten virtuellen Rechnern übergeben, treten die folgenden Symptome auf:

Symptom 1

Sicherungsjobs schlagen fehl, und folgende Meldung wird im Aktivitätsprotokoll angezeigt:

```
Failed to take snapshot. ESX/vCenter report error. A general system error occurred.
Protocol error from VMX.
```

Lösung 1

Dieser Fehler ist ein VMware-Problem. Um dieses Problem zu beheben, deinstallieren Sie VMware-Tools im Gastbetriebssystem und installieren Sie sie erneut. Übergeben Sie den Job anschließend erneut.

Symptom 2

Sicherungsjobs schlagen fehl, und folgende Meldung wird im Aktivitätsprotokoll angezeigt:

```
Es konnte kein Snapshot des virtuellen Rechners aufgenommen werden.
ESX-Server/vCenter-Server melden den folgenden Fehler: Es kann kein Snapshot im
Ruhestand erstellt werden, da das Erstellen des Snapshots den zeitlichen Grenzwert
überschritten hat, E/A im fixierten virtuellen Rechner abzuhalten.
```

Lösung 2

Dieser Fehler tritt auf, wenn VSS beim Erstellen von Snapshots auf Fehler stößt. VSS kann unter den folgenden Bedingungen auf Fehler stoßen:

Ein VSS Writer befindet sich in einem instabilen Zustand.

Um die Quelle zu bestimmen und dieses Verhalten zu korrigieren, führen Sie zur Abhilfe die folgenden Schritte durch:

1. Führen Sie den Befehl "vssadmin list writers" auf der Befehlszeile des Gastbetriebssystems auf dem virtuellen Rechner durch.
2. Stellen Sie sicher, dass alle VSS Writer in gesundem Zustand sind.
3. Setzen Sie sich für Writer, die in den folgenden Status sind, mit Microsoft oder dem Anbieter des Writers in Verbindung, um Informationen zur Fehlerbehebung zu erhalten.

   ```
   state=Failed
   Last Error=No Error
   ```

   Hinweis: Ein Neustart der Writer behebt üblicherweise das Problem.

VSS ist bei der Snapshot-Erstellung auf Fehler gestoßen.

Um die Quelle zu bestimmen und dieses Verhalten zu korrigieren, führen Sie zur Abhilfe die folgenden Schritte durch:

1. Überprüfen Sie das Windows-Ereignisprotokoll im Gastbetriebssystem. Suchen Sie nach Fehlern, die ungefähr zu der Zeit, als die Sicherung startete, mit den VSS-Komponenten in Zusammenhang stehen.
2. Wenn VSS Fehler aufgrund ungenügenden Festplattenspeichers meldet, machen Sie Festplattenspeicher auf dem Volume frei, das mit dem Fehler in Verbindung gesetzt wurde.
3. Wenn VSS oder der Windows-Volsnap-Treiber Zeitüberschreitungsfehler generiert, sind die Anwendungen, die im virtuellen Rechner ausgeführt werden, sehr aktiv. Diese Aktivität hindert VSS daran, konsistente Snapshots zu erstellen. Um dem Abhilfe zu verschaffen, planen Sie Sicherungen für Zeiten, zu denen die Anwendungen weniger Ein- und Ausgabevorgänge am Volume vornehmen.
4. Wenn das Windows-Ereignisprotokoll anzeigt, dass der VolSnap-Treiber auf Fehler gestoßen ist, lesen Sie den Artikel Volume Snapshot Driver Integrity in der Microsoft-TechNet-Bibliothek, um Informationen darüber zu erhalten, wie VolSnap-Treiberfehler behoben werden können.

Wiederherstellung virtueller Rechner schlägt mit unbekannten Fehlern fehl

Gültig auf Windows-Betriebssystemen.

Symptom:

Wiederherstellung der Jobs virtueller Rechner schlägt fehl Sie können den Job "VM wiederherstellen" übergeben, doch im Aktivitätsprotokoll wird die folgende Meldung angezeigt:

```
Fehler bei der Wiederherstellung virtueller Datenträger.
```

Außerdem wird im VDDK die folgende Fehlermeldung angezeigt:

```
Unbekannter Fehler.
```

Lösung 1:

Um dieses Problem zu beheben, beachten Sie folgende Lösungsmöglichkeiten:

- Die Wiederherstellung virtueller Rechner schlägt fehl, wenn nicht genügend freien Speicherplatz im ursprünglichen Datenspeicher vorhanden ist. VDDK gibt die Meldung zurück, da es VDDK-API (gegenwärtig) nicht unterstützt, den Wert des freien Speicherplatzes im ursprünglichen Datenspeicher zu erkennen. (Der Datenspeicher ist der Speicherort, den Sie für die Wiederherstellung des virtuellen Rechners angegeben haben.) Um dieses Problem zu beheben, machen Sie im ursprünglichen Datenspeicher so viel Festplattenspeicher frei, wie für den Abschluss des Vorgang erforderlich ist, und übergeben Sie den Job erneut.
- Netzwerkstörungen und starker Netzwerkverkehr können dazu führen, dass VM-Wiederherstellungsjobs fehlschlagen. Um dieses Problem zu beheben, stellen Sie sicher, dass der Proxy-Server über das Netzwerk mit dem ESX Server- bzw. vCenter-System kommunizieren kann, und übergeben Sie den Job erneut.
- Wenn mehrere gleichzeitige Verbindungen vorliegen, die aus Jobs zur Sicherung oder Wiederherstellung von virtuellen Rechnern auf dem ESX Server- oder vCenter Server-System bestehen - wobei Verbindungen über den VMware vSphere Client stattfinden - schlagen diese Jobs möglicherweise fehl. Um dieses Problem zu beheben, beenden Sie alle unnötigen Verbindungen, und übergeben Sie den Job erneut. Weitere Informationen zur größtmöglichen erlaubten Anzahl gleichzeitiger Verbindungen finden Sie unter VMDK-Datei kann nicht geöffnet werden (siehe Seite 155).
- Prüfen Sie die Abschnitte "Tasks" (Aufgaben) und "Events" (Ereignisse) des VMware vSphere Client-Protokolls, um interne Fehler beim spezifischen virtuellen Rechner zu entdecken. Beheben Sie die internen Fehler, und übergeben Sie den Job erneut.

  Beispiel: Eine andere Anwendung bzw. ein anderer Vorgang verwendet die VMDK-Datei. Um dieses Problem zu beheben, geben Sie die Datei frei, und übergeben Sie den Job erneut.

Lösung 2:

Dieses Problem kann unter den folgenden Bedingungen auftreten:

- In VDDK wurde ein Snapshot nicht richtig bearbeitet.
- In VDDK wurde ein Snapshot nicht manuell oder nicht vom virtuellen Rechner entfernt.

Um dieses Problem zu beheben, übergeben Sie den Job erneut. Wenn der Job erneut fehlschlägt, löschen Sie den wiederhergestellten virtuellen Rechner, und übergeben Sie den Job erneut.

Bei Sicherungs- und Wiederherstellungsvorgängen im Hotadd-Transportmodus werden Datenträger nicht geladen

Gültig auf Windows-Plattformen.

Symptom:

Bei Sicherungs- und Wiederherstellungsvorgängen im Hotadd-Transportmodus können Datenträger nicht in das Proxysystem geladen werden.

Lösung:

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

1. Öffnen Sie VMware vSphere Client.

   Melden Sie sich mit administrativen Anmeldeinformationen beim ESX Server-System an.

2. Wählen Sie den virtuellen Proxy-Rechner aus, und bearbeiten Sie seine Einstellungen.

3. Entfernen Sie die Hotadd-Datenträger, die an den virtuellen Quellrechner oder den virtuellen Proxy-Rechner angefügt sind.

4. Übergeben Sie den Job erneut.

Wiederherstellungsvorgänge schlagen fehl, wenn Daten im HOTADD- oder SAN-Transportmodus wiederhergestellt werden

Gültig auf Windows-Plattformen.

Symptom:

Wiederherstellungsvorgänge schlagen fehl, wenn Daten im HOTADD- oder SAN-Transportmodus wiederhergestellt werden. Folgende Meldung wird im Aktivitätsprotokoll angezeigt:

```
Ein unbekannter Fehler ist aufgetreten. Kontaktieren Sie den Technischen Support.
```

Lösung:

Wiederherstellungsvorgänge schlagen im HOTADD-Transportmodus (siehe Seite 211) oder im SAN-Transportmodus (siehe Seite 212) fehl, wenn die Datenträgereinstellungen nicht ordnungsgemäß konfiguriert sind.

Führen Sie folgende Schritte aus, um den Datenträger zu konfigurieren:

1. Melden Sie sich über ein Konto mit Administratorrechten beim Sicherungs-Proxysystems an.
2. Öffnen Sie die Windows-Befehlszeile.
3. Geben Sie in der Befehlszeile folgenden Befehl ein:

   ```
   diskpart
   ```

   Drücken Sie die Eingabetaste.
4. Gaben Sie "SAN" ein, und drücken Sie die Eingabetaste.

   Die aktuellen SAN-Richtlinie wird angezeigt.
5. Geben Sie folgenden Befehl ein:

   ```
   SAN POLICY = OnlineAll
   ```

   Drücken Sie die Eingabetaste.

   Die SAN-Richtlinie wird so konfiguriert, dass SAN-gehostete Volumes nicht automatisch geladen werden.
6. Um das schreibgeschützte Attribut des spezifischen SAN-Datenträgers zu löschen, wählen Sie den Datenträger aus der Datenträgerliste aus, und geben Sie den folgenden Befehl ein:

   ```
   attribute disk clear readonly
   ```

   Drücken Sie die Eingabetaste.
7. Gaben Sie "exit" ein, und drücken Sie die Eingabetaste.

Der Datenträger ist nun konfiguriert, und Sie können den Job erneut übergeben.

Wenn der Job erneut fehlschlägt, laden Sie die HOTADD-Datenträger manuell über die Datenträgerverwaltung des Proxysystems.

Um die Datenträger manuell zu laden, gehen Sie wie folgt vor:

1. Melden Sie sich über ein Konto mit Administratorrechten beim Sicherungs-Proxysystems an.
2. Öffnen Sie Windows-Systemsteuerung, und doppelklicken Sie auf "Verwaltung".

   Das Fenster "Verwaltung" wird geöffnet.
3. Doppelklicken Sie in der Liste "Favoriten" auf "Computerverwaltung".

   "Computerverwaltung" wird geöffnet.

4. Erweitern Sie den Bereich "Speicherung", und klicken Sie auf "Datenträgerverwaltung".

   Die Datenträger werden angezeigt.

5. Klicken Sie mit der rechten Maustaste auf den zu entfernenden Datenträger, und klicken Sie auf "Online".

Der Datenträger ist nun geladen, und Sie können den Job erneut übergeben.

Fehler "Operating System Not Found" treten auf

Gültig auf Windows-Plattformen.

Symptom 1

Die folgende Meldung wird angezeigt, wenn Sie versuchen, das Gastbetriebssystem auf einem virtuellen Rechner zu starten, nachdem Sie den virtuellen Rechner mithilfe der Option "An einem alternativen Speicherort wiederherstellen" wiederhergestellt haben:

```
Operating System Not Found (Betriebssystem nicht gefunden)
```

Lösung 1

Das oben aufgeführte Verhalten kann auf virtuellen Rechner auftreten, die SCSI- und IDE-Geräte enthalten. Wenn dieses Problem auftritt, überprüfen Sie, wie die Datenträger auf Ihrem virtuellen Rechner konfiguriert sind, und stellen Sie sicher, dass die Startsequenz des wiederhergestellten virtuellen Rechners dieselbe ist, wie die der Quelle des virtuellen Rechners. Wenn die Startsequenz anders ist, müssen Sie das BIOS auf dem wiederhergestellten virtuellen Rechner aktualisieren, damit sie mit der Startsequenz der Quelle übereinstimmt.

Hinweis: Der erste IDE-Datenträger sollte (0:1) verwenden.

Symptom 2

Die folgende Meldung wird angezeigt, wenn Sie versuchen, das Gastbetriebssystem auf einem virtuellen Rechner zu starten, nachdem Sie den virtuellen Rechner wiederhergestellt haben:

```
Operating System Not Found (Betriebssystem nicht gefunden)
```

Lösung 2

Wenn das oben aufgeführte Problem auftritt, überprüfen Sie, wie die Datenträger auf dem virtuellen Rechner konfiguriert sind, und stellen Sie sicher, dass die Startsequenz auf dem Replikat des virtuellen Rechners dieselbe ist, wie die der Quelle des virtuellen Rechners.

Änderungen der MAC-Adresse werden nach der VM-Wiederherstellung nicht beibehalten

Gültig auf Windows-Plattformen.

Symptom:

Die MAC-Adressen der virtuellen Rechner werden nicht beibehalten, nachdem virtuelle Rechner wiederhergestellt wurden.

Lösung:

MAC-Adressen werden während der Wiederherstellung nicht beibehalten, um Duplikate zu verhindern. Um MAC-Adressen beizubehalten, legen Sie folgenden Registrierungsschlüssel auf dem Proxy-Server fest:

```
Speicherort: SOFTWARE\CA\CA ARCSERVE D2D
Schlüsselname: RetainMACForVDDK
Werttyp: Zeichenfolge
Schlüsselwert: 1
```

Legen Sie auf virtuellen Rechnern mit zwei NIC-Karten den Registrierungsschlüssel "RetainMACForVDDK" fest, wenn Sie einen manuell festlegen möchten. Ansonsten werden alle Karten nach der Wiederherstellung automatisch festgelegt.

CA ARCserve D2D-Webservice schlägt auf CA ARCserve D2D-Knoten fehl

Gültig auf Windows-Plattformen.

Symptom:

Der Webservice, der auf den CA ARCserve D2D-Knoten ausgeführt wird, startet und schlägt fehl oder kann nicht starten.

Lösung:

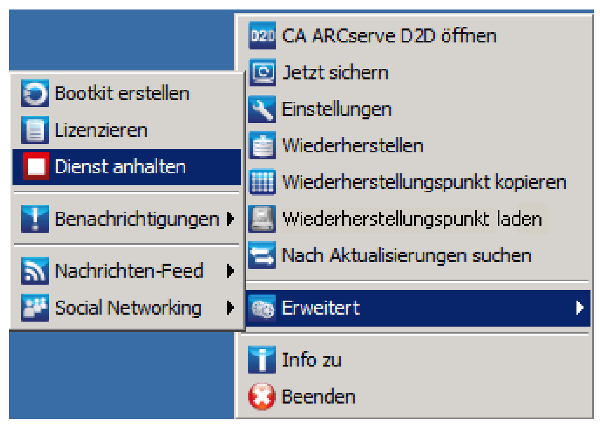
Dieses Problem tritt auf, wenn der vom CA ARCserve D2D-Webservice verwendete Port derselbe ist wie der Port, der vom VMware vCenter-Webservice (Tomcat) verwendet wird.

Der Port, den CA ARCserve D2D verwendet, kann mit dem Standardport von Tomcat im Konflikt stehen. Durch diesen Konflikt schlägt Tomcat fehl, wenn CA ARCserve D2D davor gestartet wird. Um dieses Problem zu beheben, können Sie den Standardport für Tomcat wie folgt ändern:

1. Klicken Sie im CA ARCserve D2D-Monitor auf die Option "Erweitert", und wählen Sie "Dienst anhalten".

   Der CA ARCserve D2D-Webdienst wird angehalten.



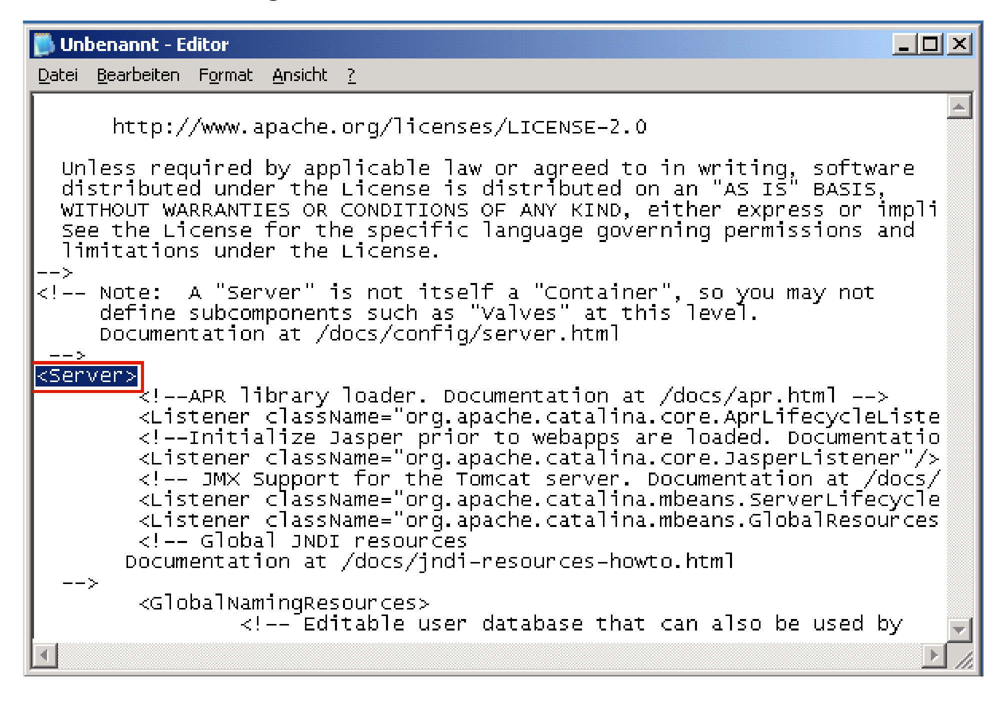


2. Öffnen Sie die Tomcat-Datei "server.xml", um das Verhalten von Tomcat zu bearbeiten bzw. zu konfigurieren.

   Die Tomcat-Datei "server.xml" ist unter der folgenden Ordnerstruktur zu finden:

   ```
   C:\Programme\CA\ARCserve Central Applications\TOMCAT\conf
   ```

3. Suchen Sie den Tag <Server> in der Datei "server.xml".



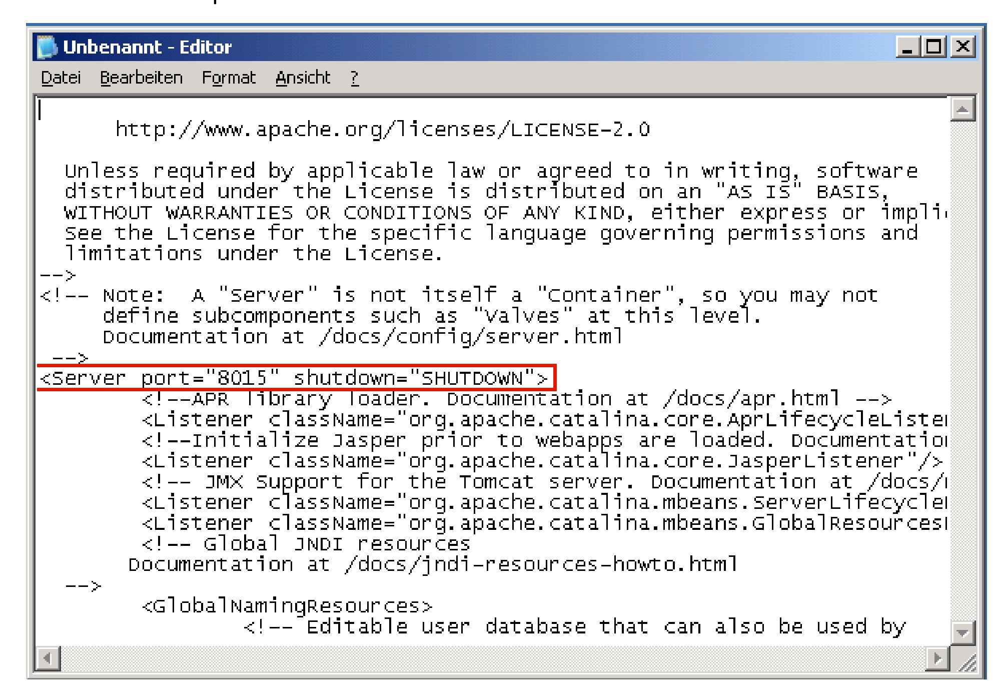
4. Bearbeiten Sie den Tag <Server> wie folgt:

   Von:

   <Server>

   In:

   <Server port="8015" shutdown="SHUTDOWN">



5. Speichern und schließen Sie die Datei "server.xml".

   Der Befehl zum Schließen von Tomcat wurde konfiguriert und kann nun vom Server auf dem genannten Port (8015) empfangen werden.

6. Klicken Sie im CA ARCserve D2D-Monitor auf die Option "Erweitert", und wählen Sie "Dienst starten".

   Der CA ARCserve D2D-Webdienst wird gestartet.

CA ARCserve Central Host-Based VM Backup kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen.

Gültig auf Windows-Betriebssystemen.

Symptom:

CA ARCserve Central Host-Based VM Backup kann keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen.

Lösung:

In der folgenden Tabelle wird beschrieben, warum CA ARCserve Central Host-Based VM Backup keine Kommunikation mit dem CA ARCserve D2D-Webservice auf Remote-Knoten herstellen kann, und enthält entsprechende Korrekturmaßnahmen:

Ursache	Korrekturmaßnahme
Das Netzwerk war bei der Anwendung der Richtlinien nicht verfügbar oder stabil.	Stellen Sie sicher, dass das Netzwerk verfügbar und stabil ist, und versuchen Sie es dann erneut.
Der CA ARCserve D2D-Computer könnte die Arbeitslast nicht verarbeiten, als die Anwendung versuchte, mit dem Knoten zu kommunizieren.	Stellen Sie sicher, dass der CPU auf dem CA ARCserve D2D-Remote-Knoten in einem Normalzustand ist, und versuchen Sie es dann erneut.
Der CA ARCserve D2D-Dienst auf dem Remote-Knoten wurde bei der Anwendung der Richtlinien nicht ausgeführt.	Stellen Sie sicher, dass CA ARCserve D2D auf dem Remote-Knoten ausgeführt wird, und versuchen Sie es dann erneut.
Die Kommunikation des CA ARCserve D2D-Diensts funktionierte nicht richtig.	Starten Sie den CA ARCserve D2D-Dienst auf dem Remote-Knoten neu, und versuchen Sie es dann erneut.

Der CA ARCserve D2D-Webservice wird nur langsam ausgeführt.

Gültig auf Windows-Betriebssystemen.

Symptom 1:

Der CA ARCserve D2D-Webservice auf CA ARCserve D2D-Systemen wird nur langsam ausgeführt. Es kann zu weiteren Symptomen kommen, wie:

- Der CA ARCserve D2D-Webservice antwortet nicht mehr oder belegt 100 Prozent der CPU-Ressourcen.
- CA ARCserve D2D-Knoten funktionieren nicht ordnungsgemäß oder können nicht mit dem Webservice kommunizieren.

Lösung 1:

In verschiedenen Umgebungskonfigurationen können Sie erkennen, dass der CA ARCserve D2D-Webservice zu viel CPU-Zeit in Anspruch nimmt oder die Reaktionszeit zu lange ist. Standardmäßig wird Tomcat konfiguriert, um den Knoten einen beschränkten Speicher zuzuweisen, der möglicherweise nicht für Ihre Umgebung geeignet sind. Um diesem Problem nachzugehen, überprüfen Sie folgende Protokolldateien:

```
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stdout.*.log
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stder.*.log
<D2D_home>\TOMCAT\logs\catalina.*.log
<D2D_home>\TOMCAT\logs\localhost.*.log
```

Suchen Sie die folgende Meldung:

```
java.lang.OutOfMemoryError
```

Um dieses Problem zu beheben, erhöhen Sie den zugewiesenen Speicher.

Führen Sie folgende Schritte aus, um den Speicher zu erhöhen:

1. Öffnen Sie den Registrierungs-Editor, und wählen Sie den folgenden Schlüssel aus:
   - x86-Betriebssysteme:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun
     2.0\CASAD2DWebSvc\Parameters\Java
     ```
   - x64-Betriebssysteme:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun
     2.0\CASAD2DWebSvc\Parameters\Java
     ```

2. Wählen Sie eine der folgenden Vorgehensweisen:
   - Wenn folgende Meldung in der Protokolldatei angezeigt wird:

     ```
     java.lang.OutOfMemoryError: PermGen space
     ```

     Hängen Sie Folgendes dem Wert der Optionen an.

     ```
     -XX:PermSize=128M -XX:MaxPermSize=128M
     ```

     Hinweis: Möglicherweise müssen Sie den Wert "-XX:MaxPermSize" erhöhen, um Ihre Umgebung anzupassen.
   - Wenn eine der folgenden Meldung in der Protokolldatei angezeigt wird:

     ```
     java.lang.OutOfMemoryError: Java heap space
     java.lang.OutOfMemoryError: GC overhead limit exceeded
     ```

     Erhöhen Sie den Wert des folgenden DWORD:

     ```
     JvmMx
     ```
3. Starten Sie den CA ARCserve D2D-Webservice neu.

Symptom 2

Geplante Sicherungen werden übersprungen und nicht mehr ausgeführt.

Lösung 2

Wenn Sie den maximalen Wert für gleichzeitige Sicherungen als 20 oder weniger konfigurieren, gehen Sie wie folgt vor:

1. Erhöhen Sie den Wert des folgenden DWORD:

   ```
   JvmMx=256
   ```

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.
2. Hängen Sie Folgendes dem Wert der Optionen an.

   ```
   -XX:MaxPermSize=128M
   ```

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.

Wenn Sie den maximalen Wert für gleichzeitige Sicherungen als über 20 aber unter 50 konfigurieren, gehen Sie wie folgt vor:

1. Erhöhen Sie den Wert des folgenden DWORD:

   ```
   JvmMx=512
   ```

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.
2. Hängen Sie Folgendes dem Wert der Optionen an.

   ```
   -XX:MaxPermSize=256M
   ```

   Hinweis: Auf diesen DWORD-Wert wird in Lösung 1 Bezug genommen.

Fehler bei der Verfolgung geänderter Blöcke

Gültig für Windows

Symptom:

Sicherungen virtueller Rechner schlagen fehl und Verfolgung geänderter Blöcke ist auf den virtuellen Rechnern aktiviert.

Lösung:

Die folgende Tabelle beschreibt Umgebungsbedingungen, die verursachen können, dass Sicherungen virtueller Rechner, bei denen die Verfolgung geänderter Blöcke aktiviert ist, fehlschlagen:

Bedingung	Lösung
Von Benutzern generierte Snapshots sind auf den virtuellen Rechnern vorhanden, und die Verfolgung geänderter Blöcke ist deaktiviert.	Aktivieren Sie oder setzen Sie die Verfolgung geänderter Blöcke zurück, damit die vollständige Sicherung fortgesetzt werden kann. **Hinweis**: Die vollständige Sicherung wird mit benutzten und unbenutzten Datenblöcken von den VMDK-Dateien fortgesetzt.
Eine falsche Version der VMware-Hardware ist auf dem virtuellen Rechner installiert.	Überprüfen Sie, dass die VMware-Hardware-Version 7.0 oder höher auf dem virtuellen Rechner installiert ist.
Eine falsche Version von ESX Server ist auf dem virtuellen Rechner installiert.	Überprüfen Sie, dass die ESX Server-Version 4.0 oder höher auf dem virtuellen Rechner installiert ist.
Das ESX Server-System ließ sich schwer herunterfahren. Schwierigkeiten beim Herunterfahren können dazu führen, dass Sicherungen von Verfolgungen geänderter Blöcke fehlschlagen.	CA ARCserve Central Host-Based VM Backup aktiviert automatisch die Verfolgung geänderter Blöcke auf dem virtuellen Rechner.
Das ESX Server-System vollzog einen (sauberen) Neustart, während der virtuelle Rechner in eingeschaltetem Status war.	CA ARCserve Central Host-Based VM Backup aktiviert automatisch die Verfolgung geänderter Blöcke auf dem virtuellen Rechner.
Der virtuelle Rechner wurde mithilfe von Storage vMotion verschoben.	CA ARCserve Central Host-Based VM Backup aktiviert automatisch die Verfolgung geänderter Blöcke auf dem virtuellen Rechner.

Sicherungen schlagen wegen ESXi-Lizenz fehl

Gültig auf Windows-Plattformen.

Symptom:

Vollständige Sicherungen, Zuwachssicherungen und Überprüfungssicherungen von CA ARCserve D2D schlagen fehl. Folgende Meldung wird im CA ARCserve D2D-Aktivitätsprotokoll angezeigt:

```
VM-Server <Servername> hat keine bezahlte ESX-Lizenz.
```

Lösung:

Aufgrund einer VMware-Einschränkung können virtuelle Rechner, die auf ESXi-Servern mit einer freien Lizenz ausgeführt werden, nicht gesichert werden. Um diese VMs zu schützen, wenden Sie eine erworbene Lizenz an.

Sicherungen schlagen fehl und Ereignis 1530 wird im Ereignisprotokoll auf dem Sicherungs-Proxy-System registriert.

Gültig auf Windows-Plattformen.

Symptom:

CA ARCserve Central Host-Based VM Backup-Jobs schlagen fehl. Ereignis 1530 wird im Anwendungs-Ereignisprotokoll auf dem Sicherungs-Proxy-System registriert.

Umgebung/Schritte, die reproduziert werden müssen:

- Microsoft SQL Server oder Microsoft Exchange Server wird auf dem virtuellen Rechner installiert.
- Der Benutzer meldet sich beim CA ARCserve Central Host-Based VM Backup-Proxy-Server mit dem Administratorkonto oder einem Konto, das Mitglied der Administratorengruppe ist, an, oder ist bereits angemeldet.
- Nachdem der Sicherungsjob gestartet wurde, meldet sich der Benutzer vom Proxy-Server ab.
- Der Sicherungsjob schlägt fehl. Ereignis 1530 wird in das Anwendungs-Ereignisprotokoll geschrieben.

  ```
  Warnung... Microsoft-Windows-User Profile-Dienst Keine Windows hat erkannt, dass Ihre Registrierungsdatei noch in Verwendung durch andere Anwendungen oder Dienste ist.  Die Datei wird jetzt entladen. Die Anwendungen oder Dienste, die Ihre Registrierungsdatei enthalten, funktionieren möglicherweise nicht richtig danach.
  ```

Ursache:

Windows Server 2008 enthält einen Benutzerprofil-Dienst, der Benutzerprofile entlädt, wenn Benutzer sich am Computer abmelden. Dadurch werden COM-Objekte möglicherweise nicht erstellt, was Host-Based VM Backup daran hindert, seine COM-Module abzurufen.

Lösung:

Um zu verhindern, dass Sicherungsjobs fehlschlagen, führen Sie die folgenden Schritte aus:

Hinweis: Damit diese Lösung funktioniert, müssen alle oben aufgelisteten Symptome vorhanden sein.

1. Melden Sie sich beim Host-Based VM Backup-Proxy-Server über das Administratorkonto oder ein Konto, das Mitglied der Administratorengruppe ist, an.
2. Starten Sie den Editor für lokale Gruppenrichtlinien, indem Sie "gpedit.msc" in das Dialogfeld "Ausführen" eingeben.
3. Blenden Sie im Editor für lokale Gruppenrichtlinien die Knoten "Computerkonfiguration", "Administrative Vorlagen", "System" und "Benutzerprofile" ein.
4. Doppelklicken Sie im Benutzerprofil-Verzeichnis auf **Die Registrierung der Benutzer bei der Benutzerabmeldung nicht zwangsweise entladen**, um das Dialogfeld **Die Registrierung der Benutzer bei der Benutzerabmeldung nicht zwangsweise entladen** zu öffnen.
5. Klicken Sie im Dialogfeld **Die Registrierung der Benutzer bei der Benutzerabmeldung nicht zwangsweise entladen** auf "Aktiviert" und anschließend auf "OK".

   Hinweis: Der Wert "DisableForceUnload" wird jetzt der Registrierung hinzugefügt.
6. Starten Sie den Host-Based VM Backup-Server neu.

Sicherungen schließen im NBD-Transportmodus ab, obwohl der Hotadd-Transportmodus festgelegt wurde

Gültig auf Windows-Plattformen.

Symptom:

Sicherungen schließen im NBD-Transportmodus (siehe Seite 211) ab, obwohl der Hotadd-Transportmodus (siehe Seite 211) für die Sicherung festgelegt wurde.

Lösung:

Mit CA ARCserve Central Host-Based VM Backup können Sie virtuelle Rechner sichern, die sich auf ESX Server-Systemen befinden. Wenn Sie virtuelle Rechner mithilfe des Hotadd-Transportmodus sichern, können Sie die einzelnen SCSI-Controller des Proxy-Servers des virtuellen CA ARCserve D2D-Rechners jeweils mit maximal 15 virtuellen Datenträgern verbinden. Wenn Sie eine Sicherung übergeben, die mehr als 15 virtuelle Datenträger enthält, und auf dem Proxy-Server des virtuellen CA ARCserve D2D-Rechners nur ein SCSI-Controller vorhanden ist, kann dieser SCSI-Controller nicht alle virtuellen Rechner unterbringen. Dies führt dazu, dass CA ARCserve Central Host-Based VM Backup die Daten im NBD-Transportmodus sichert.

Um dieses Verhalten zu vermeiden, stellen Sie sicher, dass auf dem Proxy-Server des virtuellen CA ARCserve D2D-Rechners genügend SCSI-Controller vorhanden sind, um alle virtuellen Rechner des Sicherungsjobs unterzubringen.

Zuwachssicherungsjobs werden als Überprüfungssicherungsjobs verarbeitet

Gültig für Windows

Symptom:

Wenn Sie Zuwachssicherungsjobs übergeben oder planen, die unter Verwendung des HOTADD-Transportmodus verarbeitet werden, tritt das folgende Verhalten auf:

- Die Zuwachssicherungsjobs werden in Überprüfungssicherungsjobs konvertiert. Der Aktivitätsprotokolleintrag für den Job zeigt an, dass der Zuwachssicherungsjob in einen Überprüfungssicherungsjob konvertiert wurde.
- Der Snapshot-Manager in dem VI-Client für den virtuellen Rechner, der gesichert wurde, enthält einen konsolidierten Helfer-Snapshot.
- Das Dialogfeld "Einstellungen bearbeiten" im VI-Client für den betroffenen virtuellen Rechner zeigt an, dass falsche Datenträger an das Sicherungs-Proxy-System angeschlossen sind. Die mit den falschen Datenträgern verknüpften VMDK-URLs sind nicht die gleichen wie die VMDK-URLs, die mit dem Sicherungs-Proxy-System verknüpft sind.

Lösung:

Um dieses Verhalten zu korrigieren, entfernen Sie die falschen VMDK-Dateien (Datenträger) aus dem Sicherungs-Proxy-System mithilfe der in VMware Knowlegde-Base-Artikel 1003302 beschriebenen Richtlinien. Außerdem empfiehlt VMware, dass der freie Speicherplatz auf dem Datenspeicher doppelt so groß ist wie die Gesamtgröße der Dateien des virtuellen Rechners.

Sicherungsjobs schlagen fehl, weil die Blöcke nicht identifiziert werden können

Gültig für Windows

Symptom:

Alle Sicherungsjobs eines bestimmten virtuellen Rechners schlagen fehl, und folgende Meldung wird im Aktivitätsprotokoll angezeigt:

```
Die Anwendung konnte die Blöcke, die auf dem virtuellen Rechner verwendet oder geändert wurden, nicht identifizieren. Dieses Problem kann auftreten, wenn das ESX-Server-System neu gestartet wird, während der virtuelle Rechner ausgeführt wird. Bei der nächsten Ausführung eines Sicherungsjobs wird die Anwendung die Verfolgung geänderter Blöcke zurücksetzen und eine Überprüfungssicherung durchführen.
```

Lösung:

Um dieses Verhalten zu korrigieren, führen Sie auf dem virtuellen Rechner eine Datenträgerkonsolidierung aus. Um Datenträgerkonsolidierung auszuführen, folgen Sie diesen Schritten.

1. Öffnen Sie den VMware-VI-Client.
2. Erweitern Sie das ESX Server-System für den betroffenen virtuellen Rechner.
3. Klicken Sie mit der rechten Maustaste auf den betroffenen virtuellen Rechner, wählen Sie den Snapshot aus und klicken Sie dann im Pop-up-Menü auf "Konsolidieren", um die Datenträger zu konsolidieren.
4. Übergeben Sie den Sicherungsjob erneut.

VMDK-Datei kann nicht geöffnet werden

Gültig auf Windows-Plattformen.

Symptom:

Mehrere gleichzeitige Sicherungsjobs im NBD-Transportmodus (oder LAN) schlagen fehl. Folgende Meldung wird im Aktivitätsprotokoll angezeigt:

```
VMDK-Datei kann nicht geöffnet werden
```

Lösung:

Dies ist eine VMware-Verbindungsbeschränkung. Folgende Protokollbeschränkungen der Netzwerkdateikopie (NFC) gelten für:

- ESX 4: maximal 9 Direktverbindungen
- ESX 4 über vCenter-Server: maximal 27 Verbindungen
- ESXi 4: maximal 11 Direktverbindungen
- ESXi 4 über vCenter-Server: maximal 23 Verbindungen

Darüber hinaus können Verbindungen nicht über Datenträger gemeinsam genutzt werden. Die Werte für "Maximale Beschränkungen" beziehen sich nicht auf SAN- und Hotadd-Verbindungen. Wenn der NFC-Client nicht ordnungsgemäß heruntergefahren wird, können Verbindungen für zehn Minuten offen bleiben.

Knoten werden nach einer Namensänderung nicht mehr im Bildschirm "Knoten" angezeigt

Gültig auf Windows-Plattformen.

Symptom:

Der Hostname des Knotens wurde geändert, nachdem er zum Fenster "Knoten" hinzugefügt wurde. Der Knoten wird nicht mehr im Fenster "Knoten" angezeigt.

Lösung:

Dieses Verhalten ist normal. CA ARCserve Central Host-Based VM Backup behält den Namen des Knotens, der über das Knotenfenster hinzugefügt wurde. Wenn Sie den Knoten umbenennen, kann die Anwendung den Knoten nicht erkennen. Der Knoten wird nicht im Fenster "Knoten" angezeigt.

Um umbenannte Knoten im Fenster "Knoten" anzuzeigen, gehen Sie folgendermaßen vor:

1. Benennen Sie den Knoten um.
2. Öffnen Sie den Bildschirm "Knoten" und löschen Sie den Knoten, (siehe Seite 52) der umbenannt wurde.
3. Knoten hinzufügen mithilfe seines neuen Namens.

Beim Speichern oder Zuweisen einer Richtlinie auf einen CA ARCserve D2D-Server tritt ein "Multiple Connections"-Fehler auf

Gültig für alle Windows-Plattformen.

Symptom:

Wenn Sie versuchen, eine Richtlinie auf einem CA ARCserve D2D-Server zu speichern oder sie ihm zuzuweisen, wird die folgende Fehlermeldung angezeigt:

```
Validieren des Sicherungsziels ist fehlgeschlagen. Mehrere Verbindungen zu einem Server oder eine freigegebene Ressource vom gleichen Benutzer mithilfe mehr als eines Benutzernamens zu verwenden, ist nicht zulässig. Trennen Sie alle vorherigen Verbindungen zum Server oder freigegebene Ressourcen und versuchen Sie es erneut.
```

Lösung:

Falls die vorausgehende Meldung angezeigt wird, wenn Sie versuchen, eine Richtlinie auf einem CA ARCserve D2D-Server zu speichern oder sie ihm zuzuweisen, können Ihnen die folgenden Korrekturmaßnahmen dabei helfen, das Problem zu lösen:

- Geben Sie das Feld "Benutzernamen" mit "Rechnername (oder Domänenname)\Benutzername" an.
- Gehen Sie zum Remote-Server, auf dem der freigegebene Ordner gehostet wird, und löschen Sie alle Sitzungen aus dem CA ARCserve Central Applications-Server oder CA ARCserve D2D-Server. Wählen Sie eine der folgenden Vorgehensweisen, um die Sitzungen zu löschen:
  - Führen Sie folgende Befehlszeile aus:

    ```
    net session \\machinename /delete
    ```
  - Gehen Sie zum folgenden Verzeichnis, um die Sitzung zu unterbrechen:

    ```
    Compmgmt.msc > Systemprogramme > Freigegebene Ordner > Sitzungen > Sitzung trennen
    ```
- Bestätigen Sie, dass Sie den gleichen Benutzernamen verwenden, um auf den freigegebenen Remote-Ordner zuzugreifen.
- Speichern Sie und stellen Sie die Richtlinie erneut bereit.

Sicherungen virtueller Rechner schlagen fehl, da ESX Server nicht zugreifbar ist

Gültig auf Windows-Plattformen.

Symptom:

Sicherungen virtueller Rechner schlagen fehl. Folgende Meldung wird im Aktivitätsprotokoll angezeigt:

```
Fehler bei der Erstellung eines Snapshot des virtuellen Rechners.
```

Lösung:

Sicherungen virtueller Rechnerkönnen fehlschlagen, wenn mehrere Sicherungen gleichzeitig auf einem ESX Server-System ausgeführt werden. Wenn mehrere Sicherungen gleichzeitig auf verschiedenen ESX Server-Systemen ausgeführt werden, tritt dieses Problem nicht auf. Um die virtuellen Rechner zu sichern, nimmt CA ARCserve Central Host-Based VM Backup einen Snapshot der Daten auf, die sich auf den virtuellen Rechnern befinden. Wenn mehrere Snapshot-Vorgänge gleichzeitig auf einem System ausgeführt werden, hört das ESX Server-System möglicherweise auf, zu reagieren. Obwohl das ESX Server-System nur vorübergehend anhält, wird die Sicherung unterbrochen und schlägt fehl.

Damit keine Sicherungen fehlschlagen, verwenden Sie die Lösung, die zu Ihrer Umgebung passt:

- Reduzieren Sie die Anzahl der virtuellen Rechner, die Sie gleichzeitig sichern. Wenn Sie acht virtuelle Rechner gleichzeitig sichern, reduzieren Sie die Anzahl z. B. auf sieben virtuelle Rechner, übergeben Sie die Sicherung erneut, und analysieren Sie danach die Ergebnisse. Reduzieren Sie im Bedarfsfall die Anzahl der virtuellen Rechner, die gesichert werden, bis keine Sicherungen mehr fehlschlagen oder die obige Meldung nicht im Aktivitätsprotokoll angezeigt wird.

  Um die Anzahl der virtuellen Rechner in einer Sicherung zu reduzieren, müssen Sie die Zuweisung der Richtlinie für die zu entfernenden virtuellen Rechner aufheben. Weitere Informationen finden Sie unter Aufheben der Richtlinienzuweisung für virtuelle Rechner.

- Definieren Sie eine Beschränkung der Anzahl gleichzeitiger Sicherungen. Diese Vorgehensweise hilft Ihnen dabei, die Anzahl der Sicherungsjobs zu steuern, die gleichzeitig in Ihrer Umgebung ausgeführt werden können. Weitere Informationen finden Sie unter Definieren einer Beschränkung der Anzahl von gleichzeitigen Sicherungen (siehe Seite 199).

Die Verknüpfung zum Hinzufügen neuer Registerkarten wird in Internet Explorer 8 und 9 und in Chrome nicht ordnungsgemäß geöffnet

Gültig für Windows

Symptom:

Wenn ich eine neue Registerkartenverknüpfung unter Angabe einer HTTPS-URL hinzufüge, wird folgende Fehlermeldung angezeigt, wenn ich auf die neue Registerkarte klicke:

- Internet Explorer 8 oder 9:

  `Der Inhalt wurde geblockt, da er nicht mit einem gültigen Sicherheitszertifikat signiert wurde.`

- Chrome:

  `The webpage is not available.`

Lösung:

Um dieses Problem für Internet Explorer zu beheben, gehen Sie folgendermaßen vor:

- Internet Explorer 8

  Klicken Sie auf die Statusleiste, und aktivieren Sie "Geblockte Inhalte anzeigen".

- Internet Explorer 9

  Klicken Sie auf der Statusleiste im unteren Bereich der Seite auf die Schaltfläche "Inhalt einblenden". Die Seite wird aktualisiert, und die hinzugefügte Registerkartenverknüpfung funktioniert.

Um dieses Problem für Chrome zu beheben, gehen Sie folgendermaßen vor:

Schritt 1 - Zertifikat exportieren:

1. Öffnen Sie eine neue Registerkarte in Chrome, und geben Sie die HTTPS-URL ein.

   Folgende Warnmeldung wird angezeigt: "Das Sicherheitszertifikat der Website ist nicht vertrauenswürdig!"

2. Klicken Sie im Adressbalken auf das mit einem "X" versehene Schlosssymbol.

   Ein Pop-up-Fenster mit einer Verknüpfung namens "Zertifikatinformationen" wird geöffnet.

3. Klicken Sie auf die Verknüpfung "Zertifikatinformationen".

   Das Dialogfeld "Certificate" wird geöffnet.

4. Klicken Sie auf die Registerkarte "Details"und anschließend auf "Copy to File", um das Zertifikat auf Ihrem lokalen Computer zu speichern.

   Das Dialogfeld "Certificate Export Wizard" wird geöffnet.

5. Klicken Sie auf "Next", um das Format auszuwählen, das Sie verwenden möchten, um die Datei zu exportieren.

   Hinweis: Standardmäßig ist DER encoded binary X.509 (.CER) aktiviert.

6. Klicken Sie auf "Next", um nach einem Speicherort zu suchen, an dem Sie das Zertifikat speichern möchten.

7. Klicken Sie auf "Next", um den Zertifikatsexport-Assistenten abzuschließen, und anschließend auf "Finish".

Das Zertifikat ist nun erfolgreich exportiert.

Schritt 2 - Zertifikat importieren:

1. Öffnen Sie die Tools-Optionen von Chrome.

   Das Dialogfeld "Options" wird geöffnet.

2. Wählen Sie die Option "Details", und klicken Sie neben "HTTPS/SSL" auf Zertifikate verwalten".

   Das Dialogfeld "Certificates" wird geöffnet.

3. Klicken Sie auf "Import".

   Das Dialogfeld "Certificate Import Wizard" wird geöffnet.

4. Klicken Sie auf "Next", um nach dem Zertifikat zu suchen, das Sie auf Ihrem lokalen Computer gespeichert haben.

5. Klicken Sie auf "Next", um den Zertifikatspeicher ("Certificate Store") zu öffnen.

   Das Dialogfeld "Certificate Store" wird geöffnet.

6. Klicken Sie auf "Browse", um das Dialogfeld "Select Certificate Store" zu öffnen.

   Das Dialogfeld "Select Certificate Store" wird angezeigt:

7. Wählen Sie in der Dateiliste "Trusted Root Certification Authorities", und klicken Sie auf "OK".

   Das Dialogfeld "Certificate Store" wird angezeigt:

8. Klicken Sie auf "Next", um den Zertifikatsimport-Assistenten abzuschließen, und anschließend auf "Finish".

   Es wird eine Sicherheitswarnung angezeigt, die Sie informiert, dass Sie gerade ein Zertifikat installieren.

   Klicken Sie auf "Yes", um den Bedingungen zuzustimmen.

Die Zertifikat wurde erfolgreich importiert.

Die Verknüpfung zum Hinzufügen neuer Registerkarten, RSS-Feeds und Social Networking-Feedback werden in Internet Explorer 8 und 9 nicht ordnungsgemäß geöffnet

Gültig für Windows

Symptom:

Für eine HTTPS-URL einer CA ARCserve Central Applications-Anwendung:

Wenn ich eine neue Registerkartenverknüpfung unter Angabe einer HTTPS-URL zur Navigationsleiste hinzufüge, wird folgende Fehlermeldung angezeigt, wenn ich auf die neue Registerkarte und die Verknüpfung "Feedback" klicke:

```
Die Navigation zu der Webseite wurde abgebrochen.
```

Außerdem werden die RSS-Feeds nicht angezeigt.

Hinweis: Die Verknüpfung "Feedback" zeigt die Fehlermeldung auch dann an, wenn Sie die neu hinzugefügte Registerkartenverknüpfung nicht auswählen.

Lösung:

Um dieses Problem zu beheben, gehen Sie folgendermaßen vor:

- Internet Explorer 8

  Nachdem Sie sich angemeldet haben, klicken Sie in der Pop-up-Sicherheitswarnmeldung "Möchten Sie nur die Webseiteninhalte anzeigen, die über eine sichere Verbindung übermittelt wurden?" auf "Nein". Dadurch erlauben Sie ungesicherte Inhalte für Ihre Website.

- Internet Explorer 9

  Klicken Sie auf der Statusleiste im unteren Bereich der Seite auf die Schaltfläche "Gesamten Inhalt anzeigen". Die Seite wird aktualisiert, und die hinzugefügte Registerkartenverknüpfung funktioniert.

Bei der Verwendung einer japanischen Tastatur können in Filterfeldern keine Sternchen und Unterstriche als ein Platzhalter verwendet werden

Gültig für Windows

Symptom:

Aufgrund der unterschiedlichen Tastencodes auf US- und japanischen Tastaturen können Sie mit japanischen Tastaturen das Platzhalterzeichen (*) und andere Sonderzeichen wie z. B. Unterstriche (_) nicht in die folgenden Filterfelder eingeben:

- Dies tritt nur in Firefox ein:
  - Knoten > Gruppe hinzufügen - Feld "Knotennamenfilter"
  - Richtlinien >-Registerkarte "Richtlinienzuweisung" > Richtlinie Zuweisen und Zuweisung aufheben - Feld "Knotennamenfilter"
  - Wiederherstellung > Knoten-Explorer - Feld "Knotenname"
  - Knoten > Knoten vom Auto Discovery-Ergebnis hinzufügen > Zu schützende Knoten - Feld "Knotenname"

Lösung:

Um dies zu vermeiden, öffnen Sie ein Textbearbeitungsprogramm wie Notepad. Geben Sie die Sonderzeichen("*", "_" usw.) im Texteditor ein. Kopieren Sie die Zeichen anschließend aus dem Texteditor in das Feld.

Beim Wiederherstellen eines virtuellen Rechners wird nicht der festgelegte Transportmodus verwendet, sondern ein anderer

Gültig auf Windows-Plattformen.

Symptom:

Bei der Wiederherstellung virtueller Rechner wird ein Transportmodus verwendet, der sich von dem im Registrierungsschlüssel angegeben unterscheidet.

Lösung:

Dieses Verhalten wirkt sich auf Thin-Datenträger aus. Um dieses Problem zu beheben, folgen Sie diesen Schritten:

1. Melden Sie sich beim CA ARCserve D2D-Sicherungs-Proxy-System für die virtuellen Rechner an.
2. Öffnen Sie den Registrierungs-Editor von Windows und suchen Sie nach dem folgenden Schlüssel:

   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFRestoreDll
3. Legen Sie den Registrierungsschlüssel "EnforceTransportForRecovery" auf einen der folgenden Transportmodi fest:
   - NBD
   - NBDSSL
4. Übergeben Sie die Wiederherstellung für den virtuellen Rechner.

CA ARCserve Central Host-Based VM Backup erkennt die Volumes auf den dynamischen Festplatten nicht, wenn der virtuelle Rechner auf einem alternativen ESX-Server oder Hyper-V-Server wiederhergestellt wird

Gültig auf Windows-Plattformen.

Symptom:

Die Anwendung kann die Volumes auf den dynamischen Festplatten nicht erkennen, wenn der virtuelle Rechner auf einem alternativen ESX-Server oder Hyper-V-Server wiederhergestellt wird.

Manche Datenträger werden offline gestellt, und die entsprechenden Volumes sind nicht verfügbar, wenn der virtuelle Rechner startet.

Lösung:

Um die Volumes abzurufen, melden Sie sich beim virtuellen Standby-Rechner an und schalten Sie die Datenträger in diskmgmt.msc manuell online.

Probleme bei der Wiederherstellung von Daten bei Sicherungen mit HotAdd-Transportmodus für Datenträger mit einer Größe von über 2 TB

Symptom:

Beim Sichern von VMDK-Dateien (Virtual Machine Disk, Datenträger virtueller Rechner) mit einer Größe von über 2 TB unter Verwendung des HotAdd-Transportmodus ist die Sicherung erfolgreich, die wiederhergestellten Daten sind jedoch beschädigt.

Lösung:

Aufgrund eines bekannten Problems im VMware VDDK (Virtual Disk Development Kit) ist der Sicherungsjob erfolgreich, die wiederhergestellten Daten fallen jedoch beschädigt aus. Sie können einen der folgenden Schritte durchführen, um das Problem zu lösen:

- Konfigurieren Sie Ihren Sicherungsplan neu, damit der Sicherungsjob ohne HotAdd-Transportmodus auf einem anderen Sicherungs-Proxy ausgeführt wird.
- Richten Sie die Registrierungseinstellungen so ein, dass durchgesetzt wird, dass als Transportmodus bei Sicherungen nicht HotAdd verwendet wird. Sie können SAN oder NBD/NBDSSL verwenden.

Weitere Informationen zu diesem VMware-Problem finden Sie in der VMware-Dokumentation http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2068424.

Kapitel 6: Best Practices

Dieses Kapitel enthält folgende Themen:

Bare-Metal-Recovery eines virtuellen Rechners durchführen

Bare-Metal-Recovery wird unterstützt, wenn ein virtueller Rechner zum Zeitpunkt des Sicherungsjobs eingeschaltet ist.

Eine Bare-Metal-Recovery ist eine Wiederherstellung Ihres Computersystems "von Null", einschließlich des Betriebssystems und Softwareanwendungen, mit einer darauffolgenden Wiederherstellung von Daten und Einstellungen. Durch eine Bare-Metal-Recovery können Sie Ihren Rechner mit minimalem Aufwand vollständig wiederherstellen. Dies ist sogar auf einer anderen Hardware möglich. BMR ist möglich, da CA ARCserve D2D während der Sicherung auf Blockebene nicht nur Daten, sondern auch Informationen erfasst werden, die sich auf Folgendes beziehen:

- Betriebssystem
- Installierte Anwendungen
- Konfigurationseinstellungen
- Erforderliche Treiber

Alle Informationen, die für eine vollständige Systemwiederherstellung "von Null" benötigt werden, werden in mehreren Blöcken gesichert und im Sicherungsziel gespeichert.



CA Support: So führen Sie eine Bare-Metal-Recovery durch

YouTube: So führen Sie eine Bare-Metal-Recovery durch

Voraussetzungen für eine Bare-Metal-Recovery:

- Sie müssen über einen der folgenden Punkte verfügen:
  - Ein auf eine CD/DVD gebranntes erstelltes ISO-Image für BMR
  - Ein auf einen tragbaren USB-Stick gebranntes erstelltes ISO-Image für BMR

  Hinweis: CA ARCserve D2D verwendet ein Bootkit-Hilfsprogramm, um ein WinPE-Image und ein CA ARCserve D2D-Image zu verbinden, um ein ISO-Image für BMR zu erstellen. Dieses ISO-Image wird auf einen startfähigen Datenträger gebrannt. Sie können beide startfähigen Datenträger (CD/DVD oder USB-Stick) verwenden, um das neue Computersystem zu initialisieren und den Bare Metal Recovery-Prozess zu starten. Um sicherzustellen, dass Ihr gespeichertes Image immer die aktuellste Version ist, ist es empfehlenswert, jedes Mal, wenn Sie CA ARCserve D2D aktualisieren, ein neues ISO-Image zu erstellen.
- Sie müssen über mindestens eine vollständige Sicherung verfügen.
- Auf dem virtuellen Rechner und auf dem Quellserver, den Sie wiederherstellen, muss mindestens 1 GB RAM installiert sein.
- Um virtuelle VMware-Rechner zu virtuellen VMware-Rechnern wiederherzustellen, die auf das Verhalten eines physischen Servers konfiguriert wurden, stellen Sie sicher, dass die Anwendung "VMware Tools" auf dem virtuellen Rechner des Ziels installiert ist.

Dynamische Datenträger werden nur auf Datenträgerebene wiederhergestellt. Wenn Ihre Daten auf einem lokalen Volume eines dynamischen Datenträgers gesichert sind, können Sie diesen dynamischen Datenträger während der Bare-Metal-Recovery nicht wiederherstellen. Um in diesem Szenario eine Wiederherstellung während der BMR durchzuführen, müssen Sie eine der folgenden Aufgaben ausführen, und dann eine BMR vom kopierten Wiederherstellungspunkt aus durchführen:

- Führen Sie eine Sicherung auf einem Volume oder auf einem anderen Laufwerk durch.
- Führen Sie eine Sicherung auf der Remote-Freigabe durch.
- Kopieren Sie einen Wiederherstellungspunkt in einen anderen Speicherort.

Hinweis: Wenn Sie BMR bei mehreren dynamischen Datenträgern ausführen, kann die BMR wegen unerwarteter Fehler fehlschlagen (z. B. Fehler beim Starten, unerkannte dynamische Volumes, usw). Wenn dies auftritt, sollten Sie nur den Systemdatenträger mithilfe von BMR wiederherstellen, und dann können Sie nach dem Rechnerneustart die anderen dynamischen Volumes auf einer normalen Umgebung wiederherstellen.

Der Prozess der Bare-Metal-Recovery ist bei den beiden Arten der Erstellung des Bootkit-Images praktisch identisch.

Hinweis: Der BMR-Prozess kann keine Speicherplätze erstellen. Wenn der Quellrechner Speicherplätze hat, können Sie im Zuge der BMR keine Speicherplätze am Zielrechner erstellen. Sie können diese Volumes als normale Datenträger/Volumes wiederherstellen oder vor der Ausführung der BMR manuell Speicherplätze erstellen, um Daten in diesen Speicherplätzen wiederherzustellen.

So stellen Sie Daten mithilfe von Bare-Metal-Recovery wieder her:

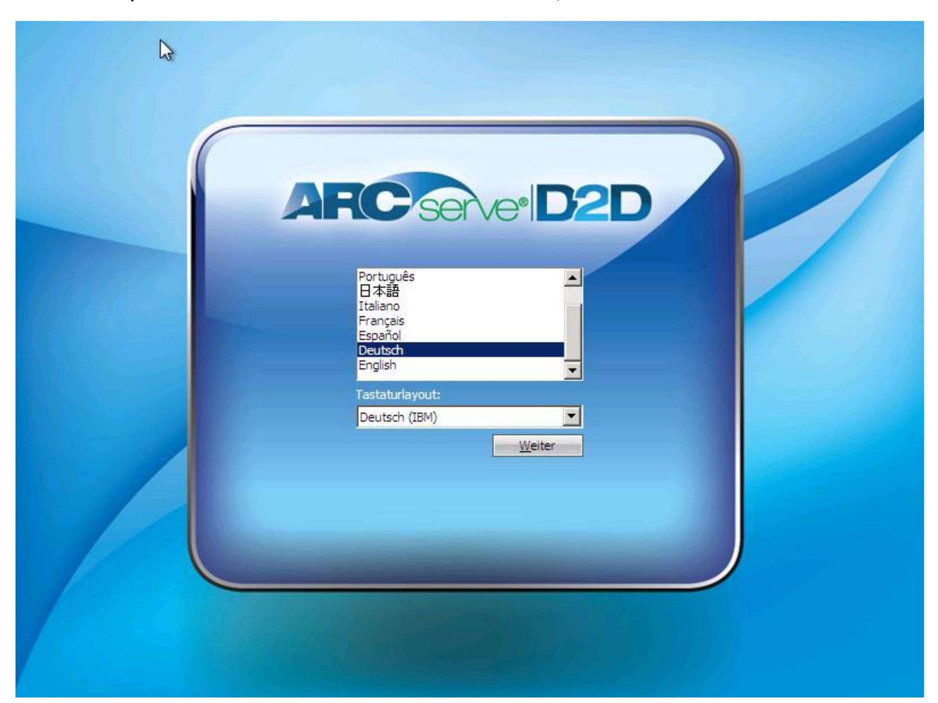
1. Legen Sie den Datenträger ein, auf dem das Bootkit-Image gespeichert ist, und starten Sie den Computer.
    - Wenn Sie ein auf eine CD/DVD gebranntes ISO-Image für BMR verwenden, legen Sie die CD/DVD ein.
    - Wenn Sie ein auf einen USB-Stick gebranntes ISO-Image für BMR verwenden, legen Sie den Stick ein.

    Der Bildschirm des BIOS-Setup-Hilfsprogramms wird angezeigt.

2. Wählen Sie im Bildschirm des BIOS-Setup-Hilfsprogramm die Option "CD-ROM Drive", um den Startprozess zu initiieren. Wählen Sie eine Architektur (x86 oder x64) aus und drücken Sie die Eingabetaste aus, um fortzufahren.



3. Der CA ARCserve D2D-Bildschirm zur Sprachauswahl wird angezeigt. Wählen Sie eine Sprache aus und klicken Sie auf "Weiter", um fortzufahren.



Die Bare-Metal-Recovery wird gestartet und der erste Bildschirm des BMR-Assistenten wird angezeigt.



CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wählen Sie einen BMR-Typ aus

Legen Sie einen Wiederherstellungstyp fest:

Gesicherte Daten mit CA ARCserve D2D wiederherstellen

(Sicherungssitzungen mit CA ARCserve D2D oder CA ARCserve Central Host-Based VM Backup).

Wiederherstellen mit einer Hyper-V-Virtual Standby-VM

(Sie können Daten nur wiederherstellen, wenn die virtuelle Konvertierung mit CA ARCserve Central Virtual Standby ausgeführt wurde)

Wiederherstellen mit einer VMware-Virtual Standby-VM

(Sie können Daten nur wiederherstellen, wenn die virtuelle Konvertierung mit CA ARCserve Central Virtual Standby ausgeführt wurde)



4. Wählen Sie vom Bildschirm des BMR-Assistenten den BMR-Typ, den Sie ausführen möchten:

   - **Gesicherte Daten mit CA ARCserve D2D wiederherstellen**

     Ermöglicht Ihnen die Wiederherstellung von Daten, die mithilfe von CA ARCserve D2D gesichert wurden. Diese Option wird in Verbindung mit Sicherungssitzungen verwendet, die mit CA ARCserve D2D oder mit der CA ARCserve Central Host-Based VM Backup-Anwendung ausgeführt werden.

     Wenn Sie diese Option auswählen, fahren Sie mit diesem Vorgang fort.

   - **Wiederherstellen mit einem virtuellen Hyper-V Virtual Standby-Rechner**

     Ermöglicht es Ihnen, Daten für einen Rechner wiederherzustellen, für den eine virtuelle Konvertierung in einen virtuellen Hyper-V-Rechner durchgeführt wurde. Diese Option wird in Verbindung mit der CA ARCserve Central Virtual Standby-Anwendung verwendet.

     Hinweis: Mit dieser Option können Sie nur Daten wiederherstellen, wenn die virtuelle Konvertierung in eine VHD-Datei (für Hyper-V) mit CA ARCserve Central Virtual Standby durchgeführt wurde.

     Wenn Sie diese Option auswählen, lesen Sie den Abschnitt Wiederherstellen mit einem virtuellen Hyper-V Virtual Standby-Rechner, um mit diesem Vorgang fortzufahren.

   - **Wiederherstellen mit einem virtuellen VMware Virtual Standby-Rechner**

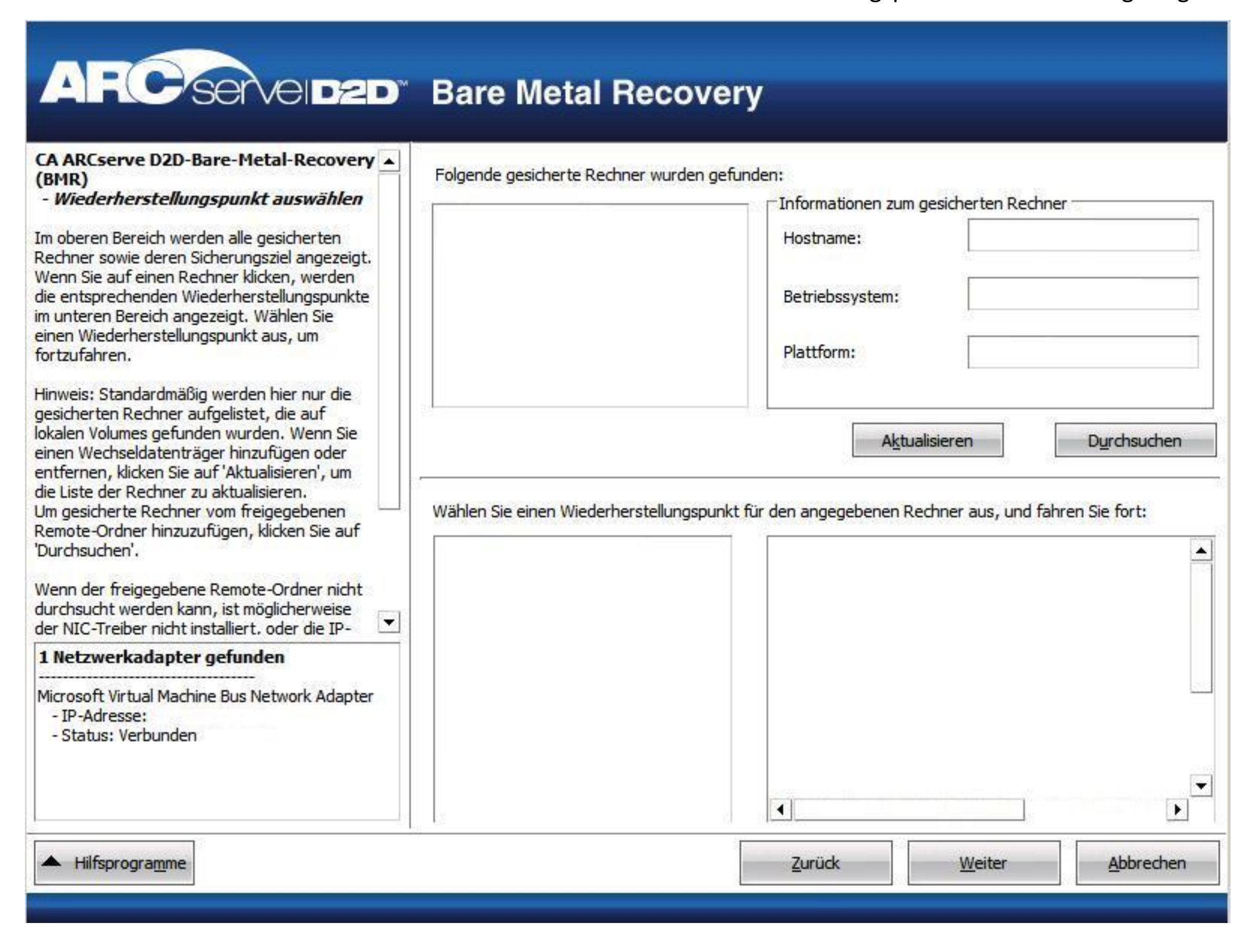
     Ermöglicht es Ihnen, Daten für einen Rechner wiederherzustellen, für den eine virtuelle Konvertierung in einen virtuellen VMware-Rechner durchgeführt wurde. Diese Option wird in Verbindung mit der CA ARCserve Central Virtual Standby-Anwendung verwendet.

     Hinweis: Mit dieser Option können Sie nur Daten wiederherstellen, wenn die virtuelle Konvertierung in eine VMDK-Datei (für VMware) mit CA ARCserve Central Virtual Standby durchgeführt wurde.

     Wenn Sie diese Option auswählen, lesen Sie den Abschnitt Wiederherstellen mit einem virtuellen VMware Virtual Standby-Rechner, um mit diesem Vorgang fortzufahren.

5. Klicken Sie auf "Weiter".

   Im Assistenten wird das Fenster "Wiederherstellungspunkt auswählen" angezeigt.



6. Wählen Sie im Fenster "Wiederherstellungspunkt auswählen" den Rechner (oder das Volume) aus, der Wiederherstellungspunkte für Ihr Sicherungs-Image enthält.

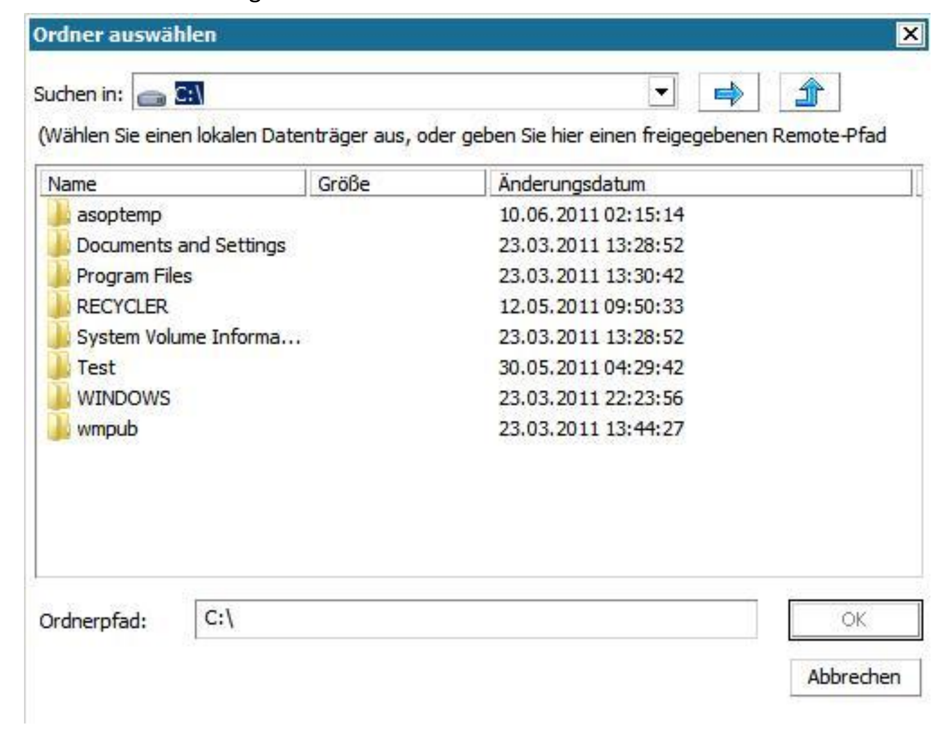
   Mit CA ARCserve D2D können Sie Wiederherstellungen von lokalen Laufwerken oder Netzwerkfreigaben durchführen.

   - Wenn Sie eine Wiederherstellung von einer lokalen Sicherung durchführen, erkennt der BMR-Assistent automatisch alle Volumes, die Wiederherstellungspunkte enthalten, und zeigt sie an.
   - Wenn Sie eine Wiederherstellung von einer Netzwerkfreigabe durchführen, suchen Sie den Remote-Speicherort der Wiederherstellungspunkte. Wenn mehrere Rechner Wiederherstellungspunkte enthalten, werden sie alle angezeigt.

     Unter Umständen benötigen Sie Zugriffsinformationen (Benutzername und Kennwort) für den Remote-Rechner.

     Hinweis: Damit Sie das Netzwerk nach den Wiederherstellungspunkten durchsuchen können, muss die Netzwerkverbindung aktiv und verfügbar sein. Über das Menü "Hilfsprogramme" können Sie gegebenenfalls Ihre Netzwerkkonfigurationsinformationen überprüfen bzw. aktualisieren sowie fehlende Treiber laden.

7. Wenn das BMR-Modul kein lokales Zielvolume entdeckt, wird das Dialogfeld "Ordner auswählen" automatisch angezeigt. Geben Sie die Remote-Freigabe an, auf der sich die Sicherungen befinden.



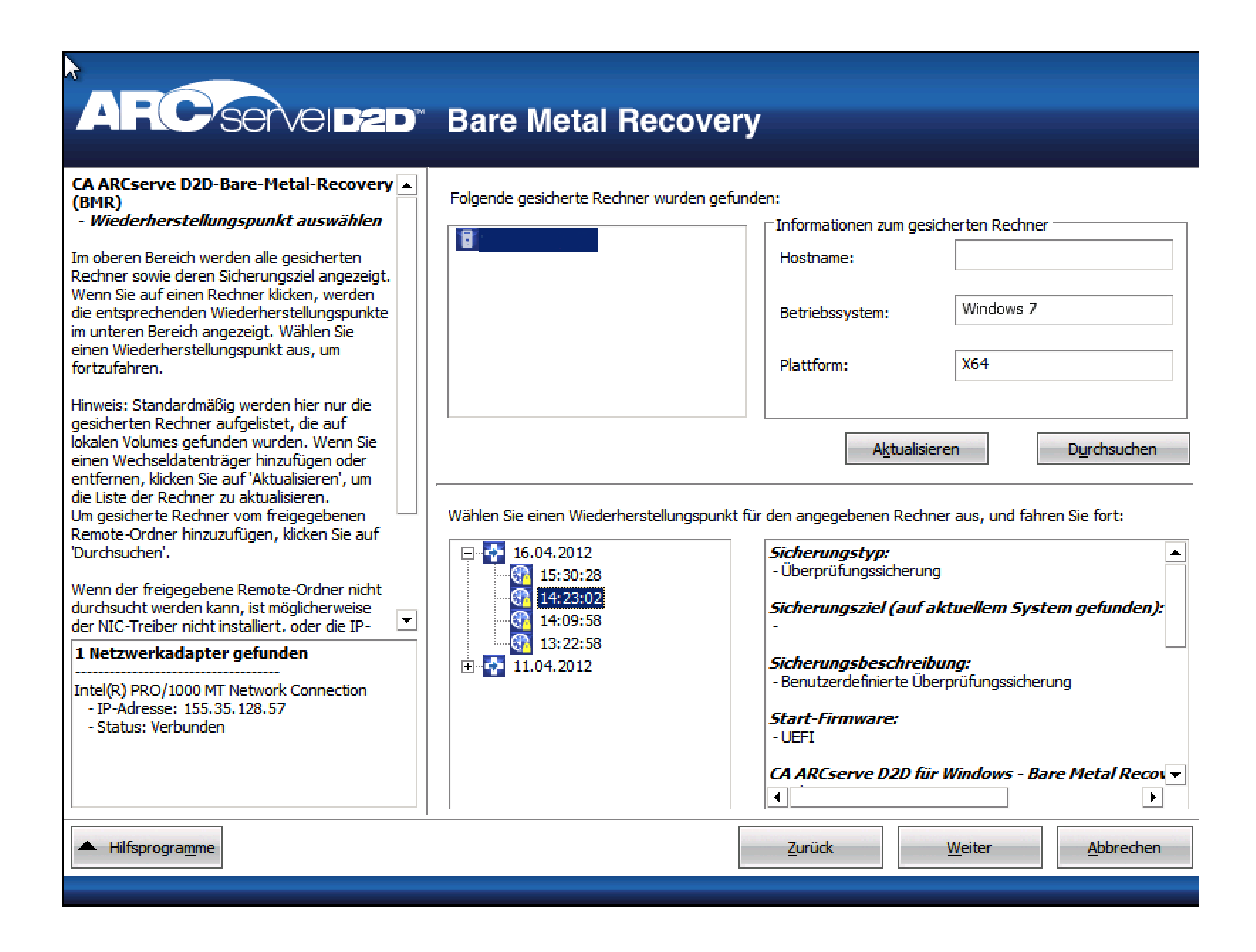
8. Wählen Sie den Ordner, in dem die Wiederherstellungspunkte für Ihre Sicherung gespeichert sind, und klicken Sie auf "OK". (Klicken Sie auf das Pfeilsymbol, um die Verbindung zum ausgewählten Speicherort zu überprüfen.)

   Der BMR-Assistent zeigt jetzt folgende Informationen an:

   - Der Rechnername (im oberen linken Bereich).
   - Die verbundenen Sicherungsinformationen (im oberen rechten Bereich).
   - Alle entsprechenden Wiederherstellungspunkte (im unteren linken Bereich).

   Hinweis: Für unterstützte Betriebssysteme können Sie BMR von Sicherungen, die auf UEFI-Rechnern durchgeführt wurden, auf BIOS-kompatible Rechner und von Sicherungen, die auf BIOS-Rechnern durchgeführt wurden, auf UEFI-kompatible Rechner durchführen. In Betriebssysteme, die UEFI/BIOS-Konvertierung unterstützen finden Sie eine vollständige Auflistung von Systemen, die die Konvertierung von Firmware unterstützen.

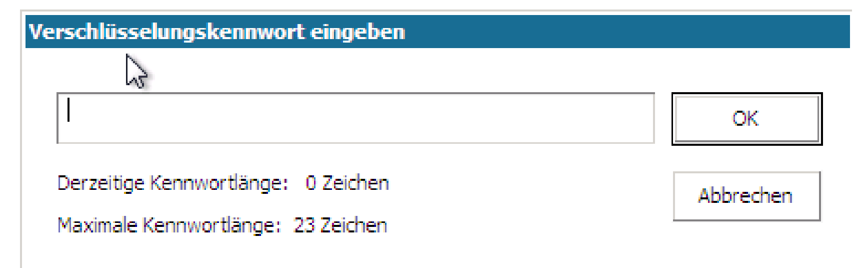
     - Für Betriebssysteme, die keine Firmwarekonvertierung unterstützen, müssen Sie den Computer in UEFI-Modus booten, um eine BMR für ein UEFI-System auszuführen. BMR unterstützt keine Wiederherstellung eines Computers mit anderer Firmware. Um zu überprüfen, ob die Start-Firmware UEFI und nicht BIOS ist, klicken Sie auf "Hilfsprogramme", "Info zu".
     - Wenn bei Betriebssystemen, die Firmwarekonvertierung unterstützen, nach der Auswahl eines Wiederherstellungspunkts entdeckt wird, dass der Quellrechner nicht die gleiche Firmware wie Ihr System ist, werden Sie gefragt, ob Sie UEFI in ein BIOS-kompatibles System oder BIOS in ein UEFI-kompatibles System konvertieren wollen.


ARCserve D2D Bare Metal Recovery
CA ARCserve D2D-Bare-Metal-Recovery (BMR)
- Wiederherstellungspunkt auswählen
Im oberen Bereich werden alle gesicherten Rechner sowie deren Sicherungsziel angezeigt. Wenn Sie auf einen Rechner klicken, werden die entsprechenden Wiederherstellungspunkte im unteren Bereich angezeigt. Wählen Sie einen Wiederherstellungspunkt aus, um fortzufahren.
Hinweis: Standardmäßig werden hier nur die gesicherten Rechner aufgelistet, die auf lokalen Volumes gefunden wurden. Wenn Sie einen Wechseldatenträger hinzufügen oder entfernen, klicken Sie auf 'Aktualisieren', um die Liste der Rechner zu aktualisieren.
Um gesicherte Rechner vom freigegebenen Remote-Ordner hinzuzufügen, klicken Sie auf 'Durchsuchen'.
Wenn der freigegebene Remote-Ordner nicht durchsucht werden kann, ist möglicherweise der NIC-Treiber nicht installiert. oder die IP-
1 Netzwerkadapter gefunden
Intel(R) PRO/1000 MT Network Connection
- IP-Adresse: 155.35.128.57
- Status: Verbunden
Folgende gesicherte Rechner wurden gefunden:
[redacted]
Informationen zum gesicherten Rechner
Hostname:
Betriebssystem: Windows 7
Plattform: X64
Aktualisieren
Durchsuchen
Wählen Sie einen Wiederherstellungspunkt für den angegebenen Rechner aus, und fahren Sie fort:
16.04.2012
15:30:28
14:23:02
14:09:58
13:22:58
11.04.2012
Sicherungstyp:
- Überprüfungssicherung
Sicherungsziel (auf aktuellem System gefunden):
-
Sicherungsbeschreibung:
- Benutzerdefinierte Überprüfungssicherung
Start-Firmware:
- UEFI
CA ARCserve D2D für Windows - Bare Metal Reco
Hilfsprogramme
Zurück
Weiter
Abbrechen

9. Wählen Sie den wiederherzustellenden Wiederherstellungspunkt aus.

   Die Informationen zum ausgewählten Wiederherstellungspunkt werden angezeigt (im rechten unteren Fensterbereich). Diese Anzeige beinhaltet Informationen wie den Typ der durchgeführten (und gespeicherten) Sicherung, das Sicherungsziel und die gesicherten Volumes.

   Wenn der Wiederherstellungspunkt verschlüsselte Sitzungen enthält (das Uhrsymbol neben dem Wiederherstellungspunkt hat eine Sperre), wird ein Bildschirm zur Kennworteingabe geöffnet. Geben Sie das Sitzungskennwort ein, und klicken Sie auf "OK".



   Hinweis: Wenn es sich bei Ihrem Rechner um einen Domänen-Controller handelt, unterstützt CA ARCserve D2D eine nicht verbindliche Wiederherstellung der Active Directory (AD)-Datenbankdatei während einer Bare-Metal-Recovery. (CA ARCserve D2D unterstützt keine Wiederherstellung von MSCS-Clustern)

10. Überprüfen Sie den gewünschten Wiederherstellungspunkt, und klicken Sie auf "Weiter".

    Im BMR-Assistenten werden die verfügbaren Wiederherstellungsmodi angezeigt.



11. Auswählen des Wiederherstellungsmodus

    Es stehen die Optionen "Erweiterter Modus" und "Express-Modus" zur Verfügung.

    - Wenn Sie den Wiederherstellungsprozess personalisieren möchten, wählen Sie "Erweiterter Modus".
    - Wenn Sie in den Wiederherstellungsprozess minimal eingreifen möchten, wählen Sie "Express-Modus".

    Standard: Express-Modus.

    Hinweis: Der restliche Vorgang gilt nur im erweiterten Modus, und der Vorgang enthält Informationen, die Sie durch die Bare-Metal-Recovery führen.

12. Klicken Sie auf "Weiter".

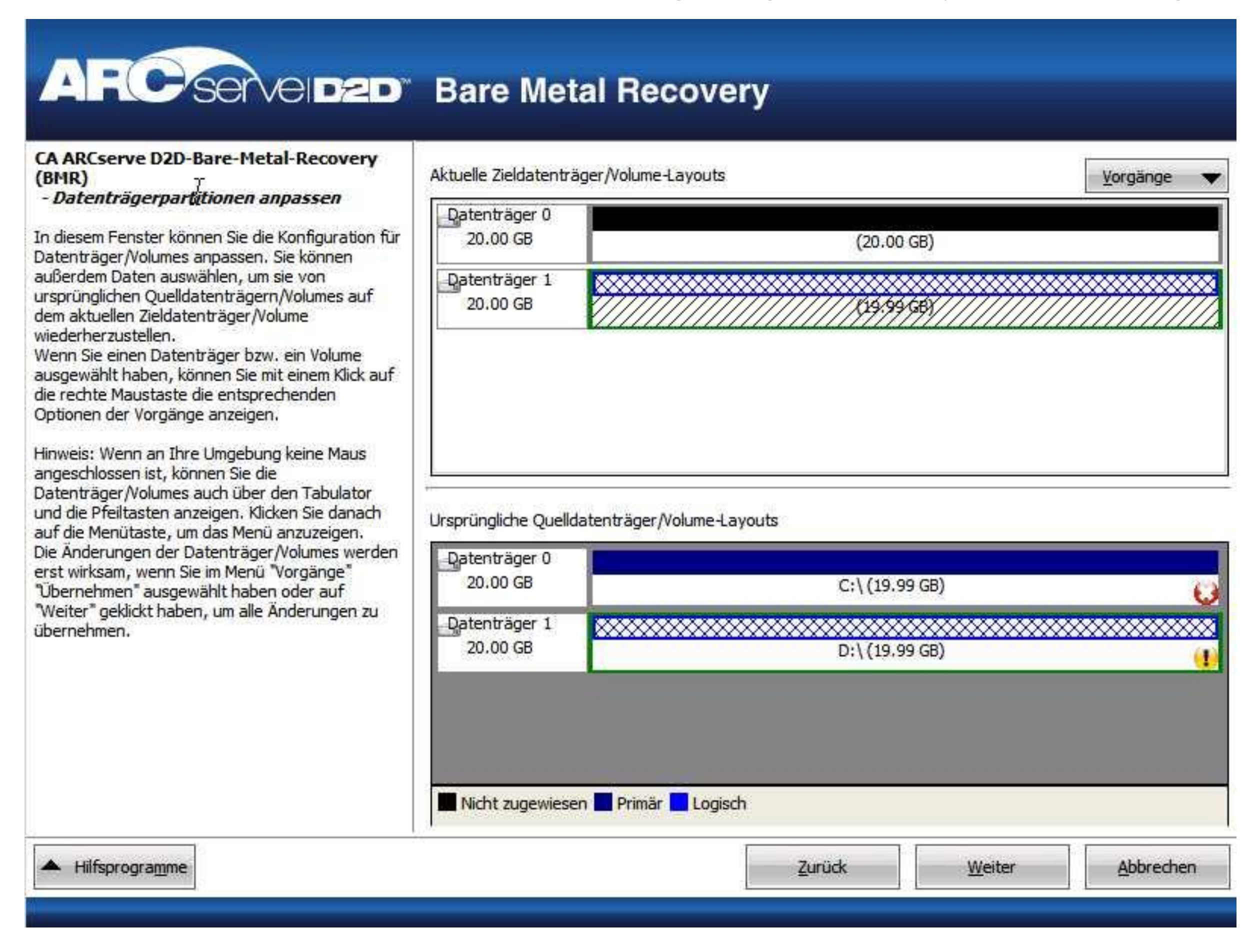
    Das BMR-Hilfsprogramm beginnt mit der Suche nach den wiederherzustellenden Rechnern und zeigt die entsprechenden Informationen zu Datenträgerpartitionen an.

    Im oberen Fensterbereich wird die Datenträgerkonfiguration des derzeitigen Rechners (Zielrechners) angezeigt. Im unteren Fensterbereich wird die Datenträgerkonfiguration angezeigt, die Sie am ursprünglichen Rechner (Quellrechner) eingestellt hatten.

Wichtig! Ein rotes X-Symbol, das für ein Quellvolume im unteren Bereich angezeigt wird, gibt an, dass dieses Volume Systeminformationen enthält und dem Zieldatenträger nicht zugewiesen (zugeordnet) wurde. Diese Systeminformationen müssen dem Zieldatenträger zugewiesen werden und während der Bare-Metal-Recovery wiederhergestellt werden. Anderenfalls schlägt der Neustart fehl.

Hinweis: Wenn Sie eine BMR ausführen und das Systemvolume auf einem Datenträger wiederherstellen, der nicht als Startdatenträger konfiguriert ist, kann der Rechner nicht gestartet werden, nachdem BMR abgeschlossen wurde. Stellen Sie sicher, dass Sie das Systemvolume auf einem ordnungsgemäß konfigurierten Startdatenträger wiederherstellen.

Hinweis: Bei einer Wiederherstellung auf einem anderen Datenträger oder Volume muss die Kapazität des neuen Datenträgers gleich oder größer als die des ursprünglichen Datenträgers/Volumes sein. Datenträger-Größenänderung ist außerdem nur bei Basisdatenträgern möglich, nicht bei dynamischen Datenträgern.

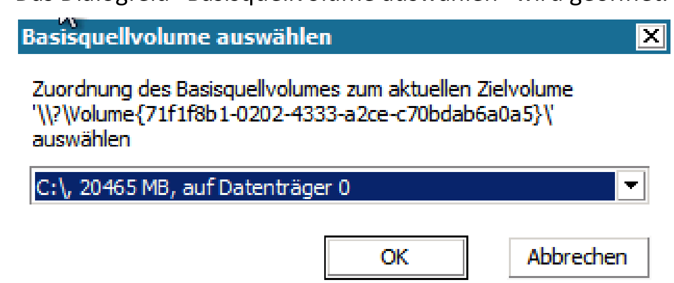


13. Wenn Ihnen die angezeigten aktuellen Datenträgerinformationen nicht richtig erscheinen, können Sie auf das Menü "Hilfsprogramm" zugreifen und nach eventuell fehlenden Treibern suchen.

14. Wenn nötig, können Sie im Fensterbereich des Zieldatenträgers/-Volume auf das Drop-down-Menü "Vorgänge" klicken, um die verfügbaren Optionen anzuzeigen. Weitere Informationen zu diesen Optionen finden Sie unter Verwalten des Menüs von BMR-Vorgängen.

15. Klicken Sie auf das entsprechende Zielvolume und wählen Sie im Popup-Menü die Option "Volume zuordnen von", um diesem Zielvolume ein Quellvolume zuzuordnen.

    Das Dialogfeld "Basisquellvolume auswählen" wird geöffnet.

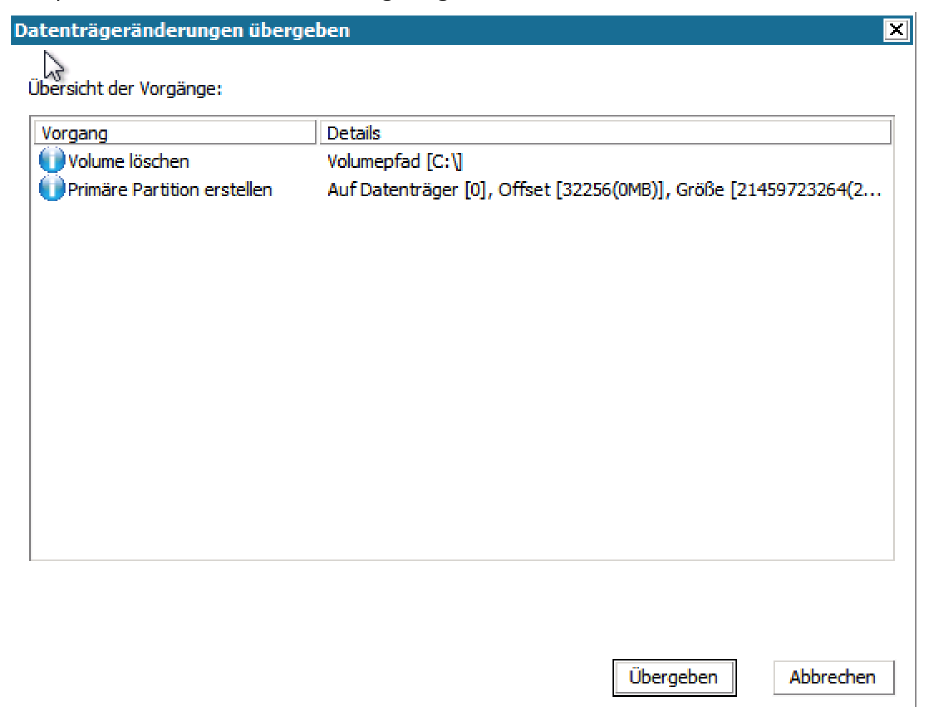
    

16. Klicken Sie im Dialogfeld "Basisquellvolume auswählen" auf das Drop-down-Menü, und wählen Sie das verfügbare Quellvolume, um es dem ausgewählten Zielvolume zuzuordnen. Klicken Sie auf "OK".

    - Im Zielvolume zeigt ein grünes hakenförmiges Symbol an, dass eine Zuordnung zu diesem Zielvolume durchgeführt wurde.
    - Im Quellvolume zeigt ein rotes x-förmiges Symbol an, dass dieses Quellvolume einem Zielvolume zugeordnet wurde.

17. Wenn Sie sicher sind, dass alle Volumes, die Sie wiederherstellen möchten, und alle Volumes, die Systeminformationen enthalten, einem Zielvolume zugeordnet sind, klicken Sie auf "Weiter".

    Im Bildschirm "Änderungen des Datenträgers übergeben" wird eine Übersicht über die ausgewählten Vorgänge angezeigt. Für jedes neu erstellte Volume werden die entsprechenden Informationen angezeigt.

18. Überprüfen Sie die Übersichtsinformationen, und klicken Sie auf "Übergeben". (Wenn die Informationen nicht richtig sind, klicken Sie auf "Abbrechen").

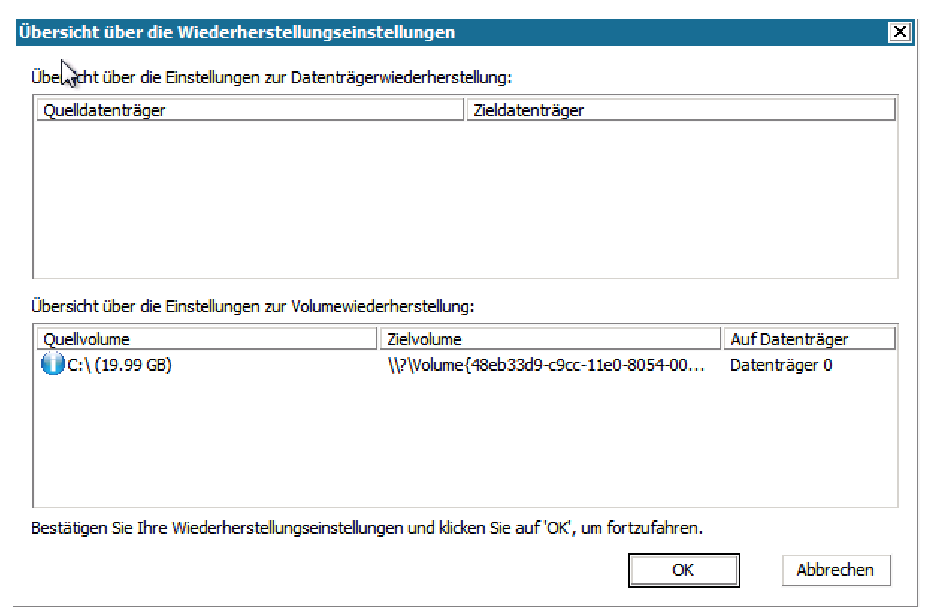
    Hinweis: Sämtliche Vorgänge, die die Festplatte betreffen, werden erst wirksam, wenn Sie sie übergeben haben.

    Auf dem Zielrechner werden die neuen Volumes erstellt und dem entsprechenden Quellrechner zugeordnet.

19. Wenn alle Änderungen abgeschlossen sind, klicken Sie auf "OK".

    Im Bildschirm "Übersicht über die Wiederherstellungseinstellungen" wird eine Übersicht der wiederherzustellenden Volumen angezeigt.

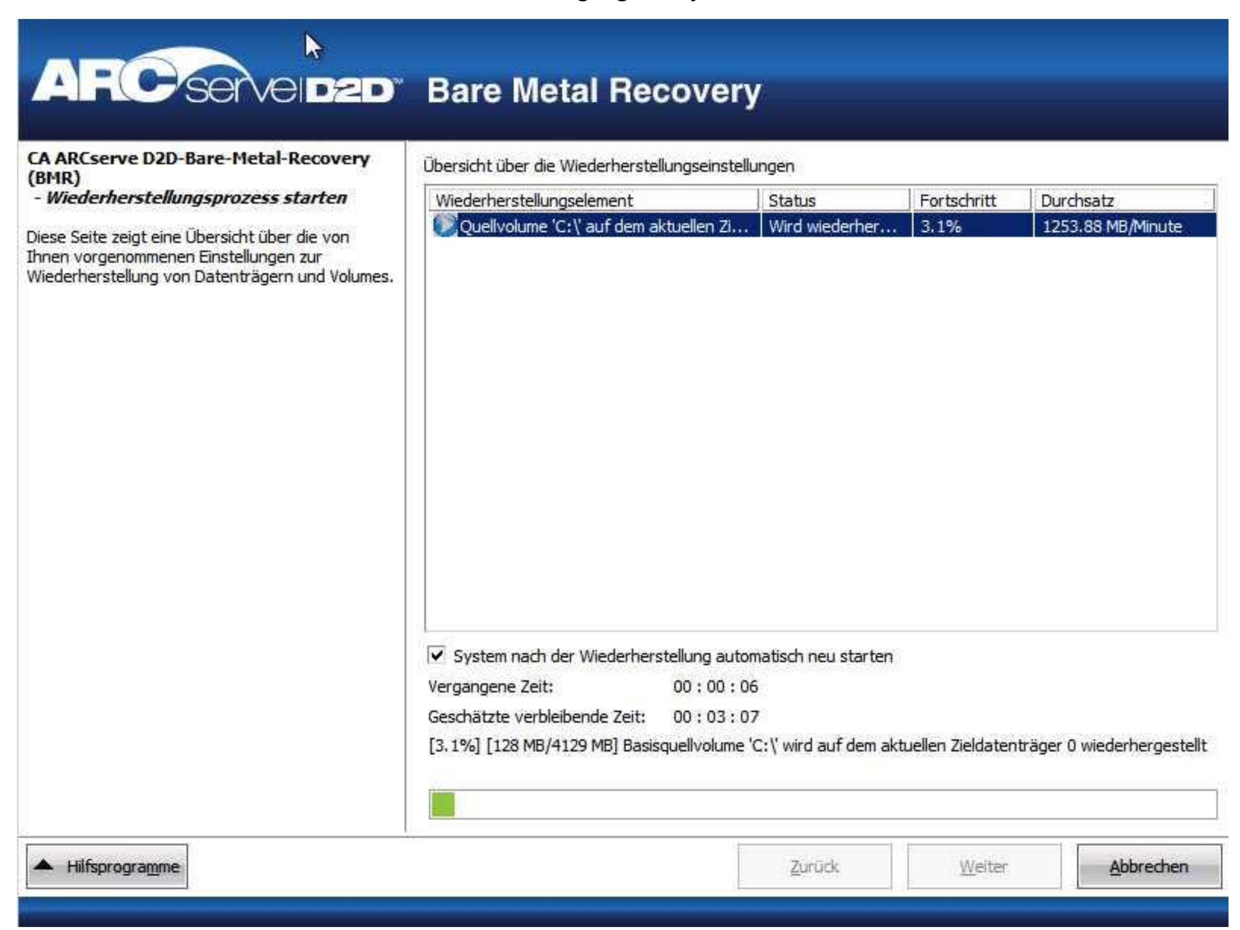
    Hinweis: Die Laufwerkbuchstaben, die unten in der Spalte "Zielvolume" aufgelistet werden, werden von Windows Preinstallation Environment (WinPE) automatisch erstellt. Sie können von den Laufwerkbuchstaben der Spalte "Quellvolume" abweichen. Auch wenn die Laufwerkbuchstaben nicht miteinander übereinstimmen werden die Daten im richtigen Volume ordnungsgemäß wiederhergestellt.



20. Nachdem Sie die Übersichtsinformationen überprüft haben, klicken Sie auf "OK".

    Der Wiederherstellungsprozess beginnt. Im BMR-Assistenten wird der Wiederherstellungsstatus jedes Volume angezeigt.

    - Dieser Vorgang kann, abhängig von der Größe des Volume, das wiederhergestellt wird, eine Weile dauern.
    - Sie stellen durch diesen Prozess sämtliche Informationen, die Sie für diesen Wiederherstellungspunkt gespeichert hatten, Block für Block wieder her und erstellen auf dem Zielrechner eine Kopie des Quellrechners.
    - Standardmäßig ist die Option, die nach der Wiederherstellung einen automatischen Systemneustart festlegt, aktiviert. Wenn nötig, können Sie diese Option löschen und den Neustart zu einem späteren Zeitpunkt manuell durchführen.
    - Sie können den Vorgang auch jederzeit abbrechen.



21. Über das Hilfsprogramm-Menü können Sie auf das BMR-Aktivitätsprotokoll zugreifen und es mit der Option "Speichern" speichern.

    Der standardmäßige Speicherplatz für das Aktivitätsprotokoll ist folgender:

    X:\windows\system32\dr\log.

    Hinweis: Wenn Sie die Option "Speichern unter" des Fensters "BMR-Aktivitätsprotokoll" verwenden, sollten Sie, um Windows-bedingten Fehlern vorzubeugen, das Aktivitätsprotokoll nicht auf dem Desktop speichern oder einen Ordner auf dem Desktop dafür erstellen.

22. Wenn Sie die Wiederherstellung auf einer abweichenden Hardware durchführen (z. B. wenn der SCSI-/FC-Adapter, der zur Verbindung mit den Festplatten verwendet wurde, geändert wurde), und im ursprünglichen System kein kompatibler Treiber gefunden wird, wird die Seite "Treibereinfügung" angezeigt, über die Sie sich mit den benötigten Treibern versorgen können.

    Sie können das System durchsuchen und einzufügende Treiber auswählen, sodass sogar ein Rechner mit anderer Hardware nach einer Bare-Metal-Recovery wiederhergestellt werden kann.

23. Nach Abschluss der Bare-Metal-Recovery wird eine Bestätigungsmeldung angezeigt.

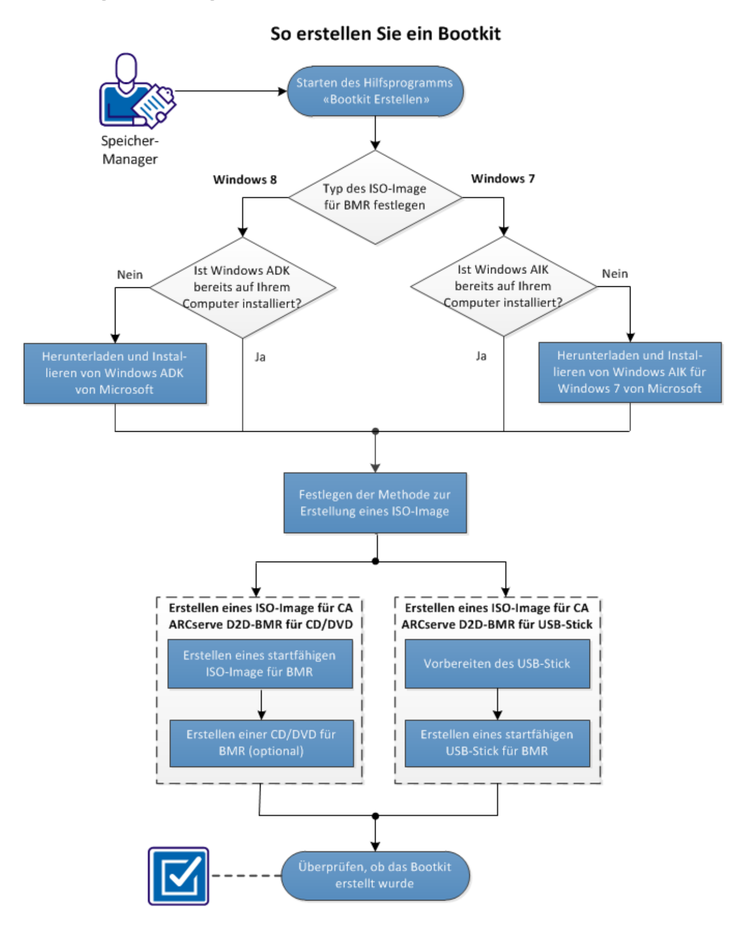
Hinweise: Nach Abschluss der BMR:

- Die erste Sicherung, die ausgeführt wird, ist eine Überprüfungssicherung.
- Wenn die Bare-Metal-Recovery abgeschlossen ist, sollten Sie überprüfen, ob das BIOS so konfiguriert ist, dass der Start vom Datenträger, auf dem das Boot-Volume wiederhergestellt wurde, durchgeführt wird.
- Wenn Sie auf abweichender Hardware wiederhergestellt haben, müssen Sie die Netzwerkadapter nach dem Neustart des Rechners möglicherweise manuell konfigurieren.
- Wenn der Rechner neu startet, wird möglicherweise ein Fenster mit einer Windows-Wiederherstellung nach einem Fehler geöffnet, das anzeigt, dass Windows nicht erfolgreich heruntergefahren ist. Wenn dies auftritt, können Sie diese Warnung beruhigt ignorieren und Windows ganz normal weiter starten.
- Bei dynamischen Datenträgern können Sie den Offline-Status des Datenträgers über die Datenträgerverwaltung manuell in online umändern (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).
- Sie können dynamische Volumes auf dynamischen Datenträgern, die aufgrund von Redundanz fehlgeschlagen sind, über die Datenträgerverwaltung manuell neu synchronisieren (führen Sie zum Zugriff auf diese Benutzeroberfläche das Steuerungshilfsprogramm Diskmgmt.msc aus).

So erstellen Sie ein Bootkit

CA ARCserve D2D verwendet ein Bootkit-Hilfsprogramm, um ein WinPE-Image (Windows Preinstallation Environment) und ein CA ARCserve D2D-Image zu verbinden, um ein ISO-Image für BMR zu erstellen. Dieses ISO-Image wird auf einen startfähigen Datenträger gebrannt. Bei einer Bare-Metal-Recovery startet der CA ARCserve D2D-Startdatenträger (CD/DVD oder USB-Stick) das neue Computersystem und ermöglicht den Beginn der Bare-Metal-Recovery.

Das folgende Diagramm veranschaulicht den Prozess für das Erstellen eines Bootkit:



Führen Sie die folgenden Aufgaben aus, um ein Bootkit zu erstellen:

1. Bootkit-Hilfsprogramm starten (siehe Seite 188)
2. Methode für das Generieren des ISO-Image für BMR festlegen (siehe Seite 191)
3. Erstellen eines CA ARCserve D2D-ISO-Image für BMR für eine CD/DVD (siehe Seite 192)
    a. Startfähiges BMR-ISO-Image erstellen (siehe Seite 192)
    b. (Optional) Erstellen einer CD oder DVD für BMR (siehe Seite 195)
4. Erstellen eines CA ARCserve D2D-ISO-Image für BMR für einen USB-Stick (siehe Seite 195)
    a. USB-Stick vorbereiten (siehe Seite 196)
    b. Startfähigen BMR-USB-Stick erstellen (siehe Seite 197)
5. Überprüfen, ob der Bootkit erstellt wurde (siehe Seite 199)

ERGÄNZENDES VIDEO

Dieser Vorgang enthält ein ergänzendes Video mit Anweisungen. Wählen Sie entweder CA Support oder YouTube als Quelle für das Anzeigen dieses Videos aus. Die Versionen des Videos von CA Support und YouTube sind identisch - nur die Anzeigequelle ist unterschiedlich:



CA Support:	So erstellen Sie ein Bootkit
YouTube:	So erstellen Sie ein Bootkit

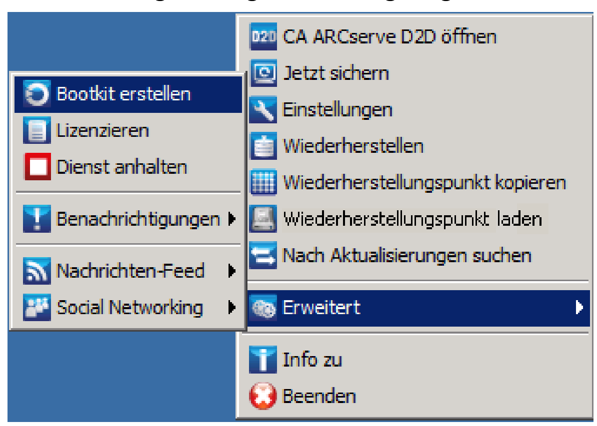
Bootkit-Hilfsprogramm starten

CA ARCserve D2D enthält das Hilfsprogramm "Bootkit-Erstellung für Bare Metal Recovery", um Ihnen dabei zu helfen, ein auf WinPE basierendes ISO-Image zu generieren. Dieses ISO-Image enthält alle Informationen, die benötigt werden, um im Bedarfsfall eine Bare-Metal-Recovery (BMR) auszuführen.

Gehen Sie wie folgt vor:

1. Sie können das Hilfsprogramm "Bootkit erstellen" in den erweiterten Optionen des Taskleistensymbols oder über das Startmenü erstellen.

   Das Hilfsprogramm "Bootkit erstellen"wird gestartet, und das Fenster "Typ des BMR-ISO-Image festlegen" wird angezeigt.

2. Geben Sie den Typ des zu erstellendem ISO-Image für BMR an (Windows 8 oder Windows 7), und klicken Sie auf "Weiter".

   Hinweis: Windows XP, Windows Vista und Windows Server 2003 werden nicht unterstützt, um ein ISO-Image für BMR zu erstellen. Für diese Betriebssysteme können Sie Windows Vista SP1, Windows 2003 SP2 oder eine spätere Version von Windows verwenden, um Ihr ISO-Image für BMR zu erstellen.

   - **Windows 8**

     Sobald es gestartet wurde, überprüft das Hilfsprogramm Ihren Computer, um zu festzustellen, ob der Windows Assessment and Deployment Kit (ADK) bereits installiert wurde. Windows ADK ist ein Microsoft-Tool, mit dem Windows-Betriebssysteme auf Computern bereitgestellt werden können.

     Hinweis: Sie können Windows ADK auf Computern mit den folgenden Betriebssystemen installieren:

     - Windows 7
     - Windows Server 2008
     - Windows Server 2008 R2
     - Windows 8
     - Windows Server 2012

   - **Windows 7**

     Sobald es gestartet wurde, überprüft das Hilfsprogramm Ihren Computer, um zu festzustellen, ob der Windows Automated Installation Kit (AIK) bereits installiert wurde. Windows AIK ist ein Microsoft-Tool, mit dem Windows-Betriebssysteme auf Computern bereitgestellt werden können.

Hinweis: Sie können Windows AIK für Windows 7 auf Computern mit den folgenden Betriebssystemen installieren:

- Windows 2003 SP2
- Windows Vista SP1
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

3. Um das startfähige ISO-Image zu erstellen, muss Windows ADK oder Windows AIK auf dem Computer installiert sein.

   a. Wenn Windows ADK (oder AIK) installiert ist, fährt das Hilfsprogramm mit dem Fenster "Bootkit-Methode auswählen" fort, damit Sie mit der Bootkit-Erstellung fortfahren können.

   b. Wenn Windows ADK (oder AIK) nicht installiert ist, wird das entsprechende Windows-Informationsfenster geöffnet. Sie müssen Windows ADK (oder AIK) vom Microsoft Download Center herunterladen und installieren.

   Hinweis: Weitere Informationen zum Installieren von Windows ADK (oder AIK) finden Sie auf den folgenden Websites:

   ■ Installieren von Windows ADK

   ■ Installieren von Windows AIK für Windows 7

   Sie können Windows ADK (oder AIK) anhand einer der folgenden Methoden installieren:

   - Laden Sie die Installationsdatenträger direkt von der Microsoft-Website herunter und installieren Sie Windows ADK (oder AIK) auf Ihrem Computer.
   - Klicken Sie auf die Links im Informationsbildschirm, um die Microsoft-Website zu öffnen, damit Sie Windows ADK (oder AIK) herunterladen und auf Ihrem Computer installieren können.

     Nachdem Sie Windows ADK (oder AIK) installiert haben, klicken Sie auf "Weiter". Das Hilfsprogramm wechselt zum Fenster "Bootkit-Methode auswählen", damit Sie mit der Bootkit-Erstellung fortfahren können.

   Hinweis: Bei Windows ADK-Installationen sind die folgenden Funktionen erforderlich, damit die Bootkit-Erstellung unterstützt wird:

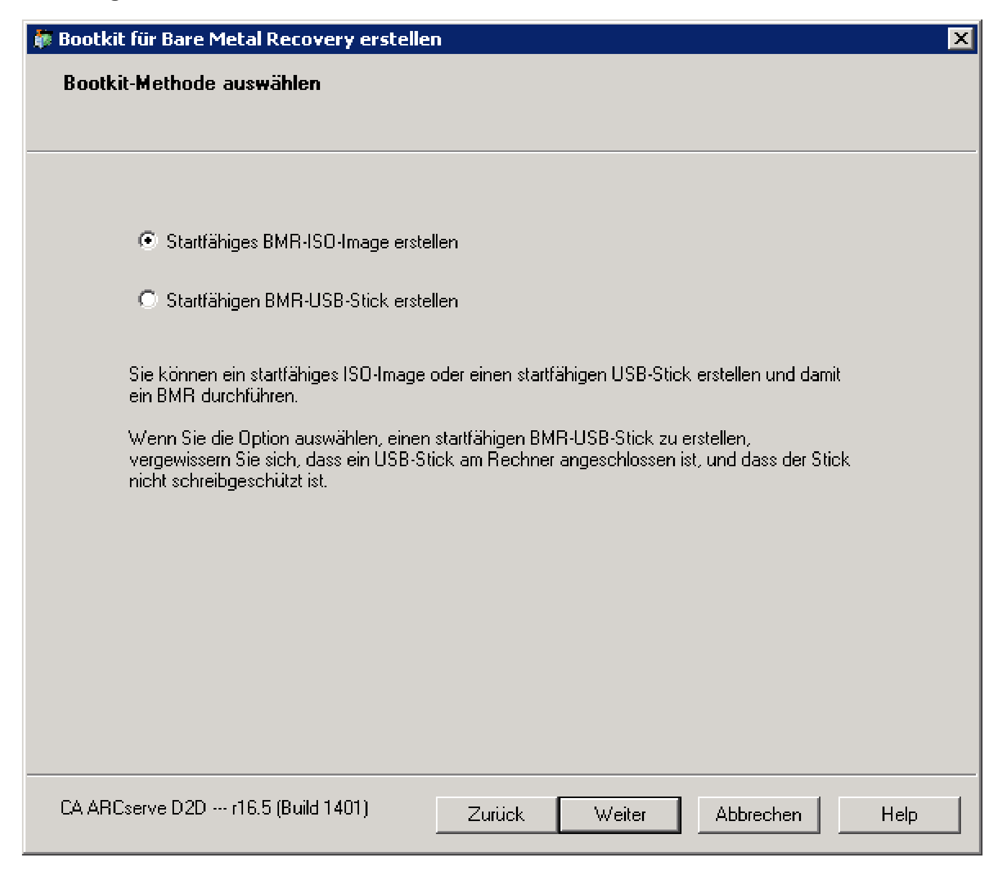
   ■ Bereitstellungstools

   ■ Windows-Vorinstallationsumgebung (Windows PE)

   Hinweis: Wählen Sie für die Installation von Windows AIK "Windows AIK-Setup" aus.

Festlegen der Methode für das Generieren des ISO-Image für BMR

Das Hilfsprogramm "Bootkit erstellen" bietet zwei Optionen für das Generieren eines ISO-Image:



- Startfähiges BMR-ISO-Image erstellen (siehe Seite 192)

  Diese Methode erstellt ein ISO-Image, das Sie auf eine CD oder DVD brennen können. Dies ist die Standardoption. Weitere Informationen finden Sie unter Erstellen eines CA ARCserve D2D-ISO-Image für BMR für eine CD/DVD (siehe Seite 192).

- Startfähigen BMR-USB-Stick erstellen (siehe Seite 197)

  Diese Methode erstellt ein ISO-Image und brennt es direkt auf einen tragbaren USB-Stick. Weitere Informationen finden Sie unter Erstellen eines CA ARCserve D2D-ISO-Image für BMR für einen USB-Stick (siehe Seite 195).

Sie können beide startfähigen Datenträger verwenden, um das neue Computersystem zu initialisieren und den Bare Metal Recovery-Prozess zu starten. Um sicherzustellen, dass Ihr gespeichertes Image immer die aktuellste Version ist, ist es empfehlenswert, jedes Mal, wenn Sie CA ARCserve D2D aktualisieren, ein neues ISO-Image zu erstellen.

Hinweis: Wenn Sie eine BMR auf einem virtuellen Rechner (VM) ausführen, können Sie das ISO-Image auch direkt an die VM anhängen, um den BMR-Prozess zu starten, ohne es zuerst auf eine CD/DVD brennen zu müssen.

Erstellen eines CA ARCserve D2D-ISO-Image für BMR für eine CD/DVD

Der Prozess für die Erstellung eines ISO-Image für CA ARCserve D2D-BMR besteht aus den folgenden Schritten:

- Startfähiges BMR-ISO-Image erstellen (siehe Seite 192)
- CD oder DVD für BMR erstellen (siehe Seite 195)

Startfähiges BMR-ISO-Image erstellen

Wenn Sie auswählen, ein ISO-Image für BMR zu erstellen, können Sie dieses Image auf einen startfähigen Datenträger (CD oder DVD) brennen, um das neue Computersystem zu initialisieren und den Bare-Metal-Recovery-Prozess zu starten.

Gehen Sie wie folgt vor:

1. Wählen Sie im Fenster "Bootkit-Methode auswählen" "Startfähiges BMR-ISO-Image erstellen", und klicken Sie auf "Weiter".

   Das Dialogfeld "Plattform und Zielspeicherort auswählen" wird geöffnet.

2. Wählen Sie die Plattform für das ISO-Image aus.

   Sie können eine oder beide der verfügbaren Optionen auswählen. Wenn Sie beide Plattformen auswählen, wird die Erstellung des mehr Zeit in Anspruch nehmen.

   Hinweis: ISO-Images, die von einer 32-Bit-Plattform erstellt werden, sollten nur zum Wiederherstellen von 32-Bit Servern verwendet werden. ISO-Images, die von einer 64-Bit-Plattform erstellt werden, sollten nur zum Wiederherstellen von 64-Bit Servern verwendet werden. Wenn Sie ein UEFI-Firmwaresystem starten wollen, stellen Sie sicher, dass die Option für x64-Plattformen aktiviert ist.

   Es sind folgende Optionen verfügbar:

   - BMR-ISO-Image für x86-Plattform (nur).
   - BMR-ISO-Image für x64-Plattform (nur).
   - BMR ISO-Image für x86- und x64-Plattformen.

3. Wählen Sie den Zielspeicherort aus.

   Geben Sie den entsprechenden Pfad an, oder durchsuchen Sie das System nach dem Speicherort für der ISO-Image-Datei für BMR.

4. Geben Sie den Namen der generierten ISO-Image-Datei für BMR an.

5. Nachdem Sie Plattform und Speicherort angegeben haben, klicken Sie auf "Weiter".

   Das Dialogfeld "Sprachen auswählen" wird geöffnet.

6. Wählen Sie die Sprache für das generierte ISO-Image für BMR aus. Während des BMR-Vorgangs werden Benutzeroberfläche und Tastatur mit der ausgewählten Sprache integriert.

   Sie können eine oder mehrere Sprachen für das BMR-ISO-Image auswählen. Allerdings führen mehrere Sprachen zu einer verlängerten Erstellungsdauer. Je mehr Sprachen Sie auswählen, desto mehr Zeit nimmt die Erstellung in Anspruch. Deswegen sollten Sie nur die Sprachen auswählen, die Sie tatsächlich benötigen.

7. Klicken Sie auf "Weiter".

   Das Dialogfeld "Treiber festlegen" wird geöffnet.

8. Geben Sie Treiber an, um die Liste der Treiber, die in das BMR ISO-Image integriert werden sollen, aufzufüllen.

   Der Treiberbereich wird aktiviert, und Sie können zusätzliche Treiber angeben, die Sie zum ISO-Image für BMR hinzufügen oder daraus entfernen wollen.

   Hinweis: Beim Integrieren des Treibers von VirtualBox Host-Only Ethernet Adapter ins BMR-ISO-Image besteht ein möglicher Konflikt mit den Windows-ADK-Komponenten. Um den Konflikt zu vermeiden, sollte der Treiber nicht ins ISO-Image für BMR integriert werden.

   a. Lokale Treiber einschließen: Laden Sie die Treiber der lokalen kritischen Geräte (nur Oem-Treiber für NIC, FC oder SCSI) zur Treiberliste. Wenn diese Option aktiviert ist, durchsucht das Hilfsprogramm Ihren Computer nach kritischen Gerätetreibern, die zum ISO-Image für BMR für diesen Computer hinzugefügt werden müssen. Wenn kritische Gerätetreiber gefunden werden, werden sie automatisch zur Liste hinzugefügt.

   b. Treiber hinzufügen: Durchsuchen Sie das System nach zu den Treibern, die zur Treiberliste hinzugefügt werden sollen.

   c. Treiber löschen: Entfernen Sie ausgewählte Treiber, die nicht zum ISO-Image für BMR hinzugefügt werden sollen, aus der Liste.

9. Klicken Sie auf "Erstellen", um den Prozess zu starten und ein startfähiges ISO-Image für BMR zu erstellen.

   Während des Vorgangs wird der Status angezeigt.

10. Wenn der Prozess abgeschlossen ist, öffnet sich ein Bestätigungsfenster, um anzuzeigen, dass das ISO-Image für BMR erfolgreich generiert wurde. Dieses Fenster enthält auch den Speicherort und die Plattform des Image sowie einen Link zu diesem Speicherort.

CD oder DVD für BMR erstellen

Nachdem das ISO-Image erstellt und am angegebenen Ziel gespeichert wurde, müssen Sie dieses Image auf eine startfähige CD oder DVD brennen. Sie können diesen startfähigen Datenträger verwenden, um das neue Computersystem zu initialisieren und den Bare Metal Recovery-Prozess (BMR) zu starten.

So stellen Sie sicher, dass das gespeicherte ISO-Image immer auf dem aktuellsten Stand ist:

- Sie sollten jedes Mal ein neues ISO-Image erstellen, wenn Sie CA ARCserve D2D aktualisieren.
- Wenn Sie das ISO-Image auf einem Remote-Speicherort gespeichert haben, sollten Sie es nur dann auf CD/DVD brennen, wenn Sie eine BMR ausführen müssen.
- Wenn Sie CA ARCserve D2D auf mehreren Computern installiert haben, sollten Sie direkt vor der BMR-Ausführung ein neues ISO-Image (samt der entsprechenden CD/DVD) von einem vertrauenswürdigen Computer erstellen, damit das Image alle aktuellen CA ARCserve D2D-Aktualisierungen enthält.

Erstellen eines CA ARCserve D2D-ISO-Image für BMR für einen USB-Stick

Der Prozess für die Erstellung eines USB-Stick für CA ARCserve D2D-BMR besteht aus den folgenden Schritten:

USB-Stick vorbereiten (siehe Seite 196)

Startfähigen BMR-USB-Stick erstellen (siehe Seite 197)

USB-Stick vorbereiten

Bevor Sie das BMR-ISO-Image auf einen USB-Stick brennen, müssen Sie den Stick vorbereiten. Um einen startfähigen USB-Stick für BMR zu erstellen, muss der Stick aktiv gemacht werden, damit er ein System booten kann. Sie können den Befehl "DiskPart" verwenden, den Stick zu aktivieren.

Wichtig! Wenn der USB-Stick formatiert werden muss, wird dieser Prozess alle gegenwärtig auf Ihrem USB-Stick gespeicherten Daten löschen. Stellen Sie sicher, dass keine wichtigen Daten auf diesem Stick gespeichert sind, bevor Sie diesen Prozess ausführen. Wenn der USB-Stick bereits zu einem früheren Zeitpunkt formatiert wurde, wird dieser Prozess Dateien mit dem selben Namen überschreiben.

Gehen Sie wie folgt vor:

1. Öffnen Sie eine Eingabeaufforderung (mit administrativen Rechten, wenn in Ihrem BS erforderlich).
2. Geben Sie **"Diskpart"** ein, und drücken Sie die Eingabetaste.
3. Geben Sie **"List Disk"** ein, und drücken Sie die Eingabetaste.

   Eine Liste aller entdeckten Datenträger wird angezeigt. Bestimmen Sie, welcher der angezeigten Datenträger Ihr USB-Datenträger ist.
4. Wählen Sie den USB-Datenträger durch die Eingabe **"Select Disk <n>"** ("n" ist die Datenträgernummer des USB-Datenträgers), und drücken Sie die Eingabetaste.
5. Geben Sie **"Clean"** ein, und drücken Sie die Eingabetaste.

   Das System zeigt "DiskPart succeeded in cleaning the disk" an.
6. Geben Sie **"create partition primary"** ein, und drücken Sie die Eingabetaste.

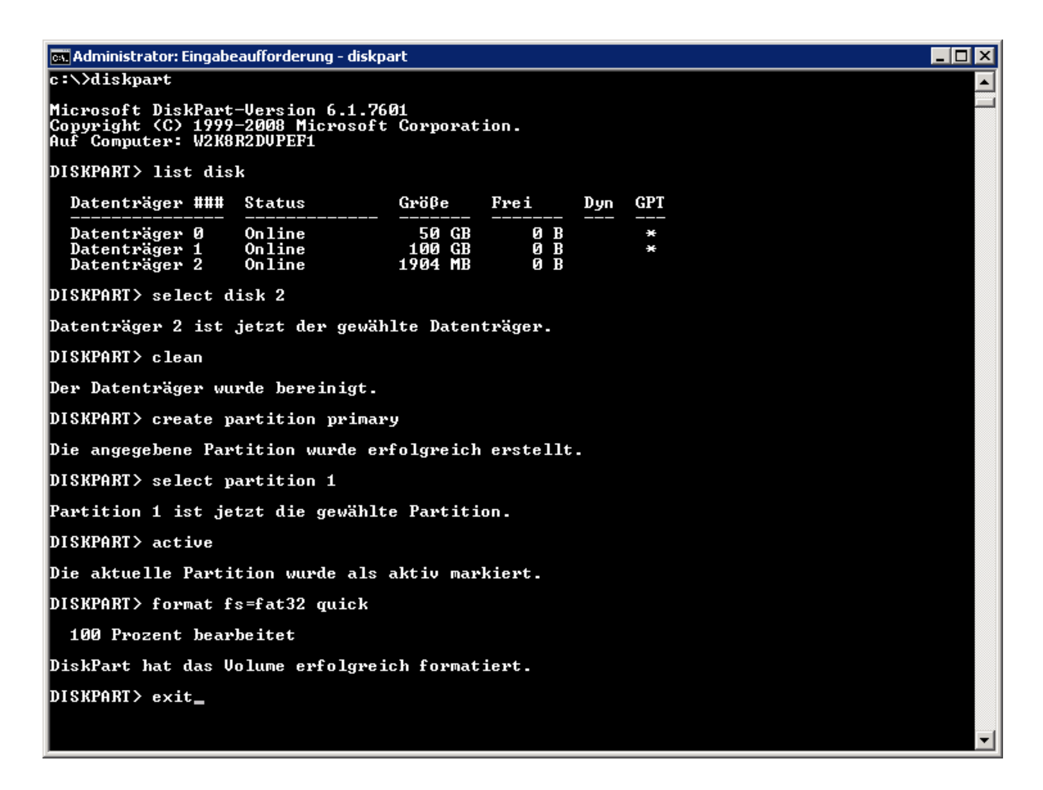
   Das System zeigt "succeeded in creating the specified partition" an.
7. Geben Sie **"select partition 1"** ein, und drücken Sie die Eingabetaste.

   Das System zeigt "Partition 1 is now the selected partition" an.
8. Geben Sie **"active"** ein, und drücken Sie die Eingabetaste.

   Das System zeigt "DiskPart marked the current partition as active" an.
9. Formatieren Sie bei Bedarf den USB-Stick mit FAT32 oder NTFS-Dateisystem.

   Geben Sie **"format fs=fat32 quick"** oder **"format fs=ntfs quick"** ein.

Der USB-Stick ist jetzt vorbereitet und bereit für die Verwendung.



Startfähigen BMR-USB-Stick erstellen

Wenn Sie auswählen, einen startfähigen USB-Stick für BMR (Bare-Metal-Recovery) zu erstellen, können Sie das ISO-Image direkt auf einen USB-Stick speichern, um das neue Computersystem zu initialisieren und den Bare-Metal-Recovery-Prozess zu starten.

Gehen Sie wie folgt vor:

1. Bereiten Sie im Bedarfsfall den USB-Stick vor. Weitere Informationen finden Sie unter USB-Stick USB-Stick vorbereiten (siehe Seite 196).
2. Wählen Sie im Fenster "Bootkit-Methode auswählen" "Startfähigen BMR-USB-Stick erstellen", und klicken Sie auf "Weiter".

   Das Dialogfeld "Plattform und Zielspeicherort auswählen" wird geöffnet.

3. Wählen Sie die Plattform für das ISO-Image aus.

   Sie können eine oder beide der verfügbaren Optionen auswählen. Wenn Sie beide Plattformen auswählen, wird die Erstellung des mehr Zeit in Anspruch nehmen.

   Hinweis: ISO-Images, die von einer 32-Bit-Plattform erstellt werden, sollten nur zum Wiederherstellen von 32-Bit Servern verwendet werden. ISO-Images, die von einer 64-Bit-Plattform erstellt werden, sollten nur zum Wiederherstellen von 64-Bit Servern verwendet werden. Wenn Sie ein UEFI-Firmwaresystem starten wollen, stellen Sie sicher, dass die Option für x64-Plattformen aktiviert ist.

   Es sind folgende Optionen verfügbar:

   - BMR-ISO-Image für x86-Plattform (nur).
   - BMR-ISO-Image für x64-Plattform (nur).
   - BMR ISO-Image für x86- und x64-Plattformen.

4. Geben Sie das Laufwerk des USB-Stick an.

   Geben Sie das Laufwerk an, an dem die ISO-Image-Datei für BMR erstellt und auf den USB-Stick gespeichert werden soll, oder durchsuchen Sie das System danach.

   Hinweis: Wenn Sie das UEFI-Firmwaresystem starten möchten, sollten Sie den USB als FAT32-Dateisystem formatieren.

5. Stellen Sie sicher, dass ein vorbereiteter USB-Stick ins angegebene Laufwerk eingefügt wurde.

6. Nachdem Sie Plattform und Speicherort angegeben haben, klicken Sie auf "Weiter",

   Das Dialogfeld "Sprachen auswählen" wird geöffnet.

7. Wählen Sie die Sprache für das generierte ISO-Image für BMR aus. Während des BMR-Vorgangs werden Benutzeroberfläche und Tastatur mit der ausgewählten Sprache integriert.

   Sie können eine oder mehrere Sprachen für das BMR-ISO-Image auswählen. Allerdings führen mehrere Sprachen zu einer verlängerten Erstellungsdauer. Je mehr Sprachen Sie auswählen, desto mehr Zeit nimmt die Erstellung in Anspruch. Deswegen sollten Sie nur die Sprachen auswählen, die Sie tatsächlich benötigen.

8. Klicken Sie auf "Weiter".

   Das Dialogfeld "Treiber festlegen" wird geöffnet.

9. Wählen Sie bei Bedarf die Option für die Integration zusätzlicher Treiber aus.

   Der Treiberbereich wird aktiviert, und Sie können zusätzliche Treiber angeben, die Sie zum ISO-Image für BMR hinzufügen oder daraus entfernen wollen.

10. Klicken Sie auf "Erstellen", um den Prozess zu starten und ein startfähiges ISO-Image für BMR zu erstellen.

    Während des Vorgangs wird der Status angezeigt.

11. Wenn der Prozess abgeschlossen ist, wird ein Bestätigungsfenster geöffnet, um anzuzeigen, dass das BMR ISO-Image erfolgreich generiert und auf Ihren USB-Stick gespeichert wurde. Dieses Fenster enthält auch den Speicherort und die Plattform des Image sowie einen Link zu diesem Speicherort.

Überprüfen, ob der Bootkit erstellt wurde

Wenn das ISO-Image für BMW erfolgreich erstellt wurde, wird im Hilfsprogramm "Bootkit erstellen" ein Link zum Speicherort des Image angezeigt. Stellen Sie sicher, dass das ISO-Image für BMR an diesem Speicherort gespeichert ist. Standardmäßig wird das Image im Bibliotheks- oder Dokumentordner gespeichert, mit folgendem standardmäßigen Image-Namens-Format:

<PRODUKT>_BMR_<Plattform>_<BS Kernel>_<Version>(Build xxx).ISO

Beispiel:

D2D_BMR_x86x64_w8_r16.5 (Build 1234).ISO

Definieren einer Beschränkung der Anzahl von gleichzeitigen Sicherungen

Sie können eine Beschränkung der Anzahl an CA ARCserve D2D-Sicherungsjobs definieren, die gleichzeitig ausgeführt werden können. Diese Möglichkeit ermöglicht es Ihnen, die Proxy-Server-Leistung des virtuellen CA ARCserve D2D-Rechners in Ihrer Sicherungsumgebung zu optimieren. Standardmäßig kann Host-Based VM Backup bis zu zehn D2D-Sicherungsjobs gleichzeitig ausführen. Bei Umgebungen mit vielen virtuellen Rechnern, die einem Proxy-System des virtuellen CA ARCserve D2D-Rechners zugeordnet sind, kann sich eine große Anzahl von gleichzeitigen Sicherungen negativ auf Netzwerk- und Sicherungsleistungen auswirken.

Hinweis: Wenn die Anzahl an gleichzeitigen Jobs die angegebene Grenze überschreitet, gelangen die Jobs, die die Grenze überschreiten, in die Jobwarteschlange.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Proxysystem des virtuellen CA ARCserve D2D-Rechners an.

2. Öffnen Sie die Windows-Registrierung, und suchen Sie nach dem folgenden Registrierungsschlüssel:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE D2D
   ```

3. Klicken Sie mit der rechten Maustaste auf CA ARCserve D2D, wählen Sie "Neu" aus und klicken Sie im Pop-up-Menü auf "Zeichenfolgewert".

   Benennen Sie den Schlüssel folgendermaßen:

   `VsphereMaxJobNum`

4. Klicken Sie mit der rechten Maustaste auf "VsphereMaxJobNum", und wählen Sie im Kontextmenü die Option "Ändern" aus.

   Das Dialogfeld "Zeichenfolge bearbeiten" wird geöffnet.

5. Geben Sie im Feld "Wertdaten" die Anzahl an CA ARCserve D2D-Sicherungsjobs an, die gleichzeitig ausgeführt werden dürfen.

   - **Untergrenze:** 1
   - **Maximale Anzahl:** Keine

6. Klicken Sie auf "OK". Die Grenze ist jetzt definiert.

7. Starten Sie den CA ARCserve D2D-Webservice neu.

Erhöhen der Anzahl von Meldungen, die in der VMVixMgr-Protokolldatei aufbewahrt werden

Die VMVixMgr-Protokolldatei bewahrt Meldungen auf, die sich auf VMware-VIX-Vorgänge beziehen. Weitere Informationen über die VMware VIX-API finden Sie auf der VMware-Website.

Die VMVixMgr-Protokolldatei (VMVixMgr.log) ist im folgenden Verzeichnis auf dem Sicherungs-Proxy-System gespeichert:

```
C:\Programme\CA\ARCserve D2D\Protokolle
```

Standardmäßig kann die Protokolldatei 500 KB nicht überschreiten. Wenn die Protokolldatei 500 KB überschreitet, werden die in der Protokolldatei enthaltenen Meldungen überschrieben. Dieses Verhalten verhindert, dass die Protokolldatei 500 KB überschreitet.

Wenn Sie einen Ablaufplan definieren, um in 15- Minuten-Abständen Daten zu sichern, ist es sehr wahrscheinlich, dass die Protokolldatei überschrieben wird, sobald die Protokolldatei 500 KB überschreitet. Durch Steigerung der Protokolldateigröße können Sie mehr Meldungen in der Protokolldatei aufbewahren.

Als Best Practice empfiehlt es sich, die Protokolldatei nur dann zu vergrößern, wenn Sie einen Ablaufplan zur Datensicherung in 15-Minuten-Abständen definieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Sicherungs-Proxy-System an.
2. Öffnen Sie die Windows-Registrierung, und suchen Sie nach dem folgenden Registrierungsschlüssel:

   `HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D`

3. Klicken Sie mit der rechten Maustaste auf "CA ARCserve D2D", wählen Sie "Neu" aus und klicken Sie im Pop-up-Menü auf "DWORD-Wert"

   Benennen Sie das "DWORD" folgendermaßen:

   `VixMgrLogSize`

   Hinweis: Falls dieses DWORD nicht vorhanden ist, liegt der Standardwert für die Protokolldatei faktisch bei 500 KB.

4. Nachdem Sie das DWORD erstellt haben, klicken Sie mit der rechten Maustaste auf "VixMgrLogSize" und im Pop-up-Menü auf "Ändern", um das Dialogfeld "DWORD-WERT bearbeiten" zu öffnen.
5. Geben Sie im Feld "Datenwerte" des Dialogfelds "DWORD bearbeiten" einen Wert (in KB) für die Protokolldatei an. Zum Beispiel 750, 1000 usw.
6. Klicken Sie auf "OK", um den Wert anzuwenden und das Dialogfeld "DWORD-Wert bearbeiten" zu schließen.

Schützen des CA ARCserve D2D-Sicherungs-Proxys

Mit CA ARCserve Central Host-Based VM Backup erstellte Sicherungssitzungen werden auf dem Sicherungs-Proxy gespeichert. Abhängig von Ihrer Konfiguration können Sie den Sicherungs-Proxy selbst auf verschiedene Art und Weise schützen.

- Wenn Sie CA ARCserve Central Protection Manager ausführen, können Sie den Sicherungs-Proxy als einen zu schützenden Knoten hinzufügen. Weitere Informationen finden Sie im CA ARCserve Central Protection Manager-Benutzerhandbuch.
- Starten Sie die CA ARCserve D2D-Instanz lokal auf dem Sicherungs-Proxy und konfigurieren Sie die Sicherungseinstellungen. Wählen Sie "Gesamter Rechner" als Sicherungsquelle aus. Weitere Informationen finden Sie im CA ARCserve D2D-Benutzerhandbuch.
- Wenn Sie CA ARCserve Backup ausführen, können Sie einen Sicherungsjob konfigurieren, um den Proxy zu schützen.

Auswirkungen des Installationsprozesses auf das Betriebssystem

Durch den CA ARCserve Central Applications-Installationsprozess werden mithilfe des Installationsmoduls "Microsoft-Installationspaket" (MSI) verschiedene Komponenten des Windows-Betriebssystems aktualisiert. Mit den im MSI enthaltenen Komponenten kann CA ARCserve Central Applications benutzerdefinierte Aktionen zum Installieren oder Aktualisieren von CA ARCserve Central Applications durchführen.

In der folgenden Liste sind die benutzerdefinierten Aktionen und die betroffenen Komponenten aufgeführt.

Hinweis: Alle CA ARCserve Central Applications-MSI-Pakete rufen die in dieser Tabelle enthaltenen Komponenten auf, wenn Sie CA ARCserve Central Applications installieren.

Komponente	**Beschreibung**
CallAllowInstall	Hiermit werden beim Installationsvorgang die Bedingungen überprüft, die einen Bezug zur aktuellen Anwendungsinstallation haben.
CallPreInstall	Hiermit können beim Installationsprozess MSI-Eigenschaften gelesen und geschrieben werden. Beispielsweise kann der Installationspfad der Anwendung im MSI gelesen werden.
CallPostInstall	Hiermit können beim Installationsprozess verschiedene mit der Installation verbundene Aufgaben ausgeführt werden. Beispielsweise kann die Anwendung in der Windows-Registrierung registriert werden.

Komponente	Beschreibung
CallAllowUninstall	Hiermit werden beim Deinstallationsvorgang die Bedingungen überprüft, die einen Bezug zur aktuellen Anwendungsinstallation haben.
CallPreUninstall	Hiermit können beim Deinstallationsprozess verschiedene mit der Installation verbundene Aufgaben ausgeführt werden. Beispielsweise kann die Registrierung von der Anwendung in der Windows-Registrierung rückgängig gemacht werden.
CallPostUninstall	Hiermit werden beim Deinstallationsvorgang mehrere Aufgaben ausgeführt, nachdem die installierten Dateien deinstalliert wurden. Zum Beispiel können die restlichen Dateien entfernt werden.
ShowMsiLog	Zeigt die Protokolldatei von Windows Installer in Notepad an, wenn der Endbenutzer in den Dialogfeldern "Setup erfolgreich", "Setup fehlgeschlagen" oder "Setup unterbrochen" das Kontrollkästchen der Option "Protokolldatei von Windows Installer anzeigen" aktiviert und dann auf "Fertig stellen" klickt. (Dies funktioniert lediglich mit Windows Installer 4.0.)
ISPrint	Druckt die Inhalte eines Steuerelements mit scrollbarem Text auf einem Dialogfeld aus. Dies ist eine benutzerdefinierte Aktion der Windows-Installer-DLL. Die DLL-Datei heißt SetAllUsers.dll, und ihre Einsprungstelle ist PrintScrollableText.
CheckForProductUpdates	Verwendet FLEXnet Connect, um auf Produktaktualisierungen zu prüfen. Diese benutzerdefinierte Aktion startet eine ausführbare Datei mit dem Namen "Agent.exe" und gibt folgende Informationen weiter: /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Verwendet FLEXnet Connect, um nach dem Neustart auf Produktaktualisierungen zu prüfen. Diese benutzerdefinierte Aktion startet eine ausführbare Datei mit dem Namen "Agent.exe" und gibt folgende Informationen weiter: /au[ProductCode] /EndOfInstall /Reboot

- **Aktualisierte Verzeichnisse:** Während des Installationsvorgangs werden Anwendungsdateien standardmäßig in den folgenden Verzeichnissen installiert und aktualisiert:

  `C:\Programme\CA\`*<Anwendungsname> (beispielsweise ARCserve Central Applications oder ARCserve D2D)*

  Sie können die Anwendung im Standardinstallationsverzeichnis oder in einem alternativen Installationsverzeichnis installieren. Der Installationsprozess kopiert verschiedene Systemdateien ins folgende Verzeichnis:

  `C:\WINDOWS\SYSTEM32`

- **Aktualisierte Windows-Registrierungsschlüssel:** Der Installationsprozess aktualisiert die folgenden Windows-Registrierungsschlüssel:

  Standard-Registrierungsschlüssel:

  `HKLM\SOFTWARE\CA\`*<Anwendungsname> (beispielsweise ARCserve Central Applications oder ARCserve D2D)*

  Basierend auf der aktuellen Konfiguration Ihres Systems werden beim Installationsprozess neue Registrierungsschlüssel erstellt und verschiedene weitere Registrierungsschlüssel geändert.

- **Installierte Anwendungen:** Beim Installationsprozess werden folgende Anwendungen auf Ihrem Computer installiert:
  - CA Licensing
  - Microsoft Visual C++ 2010 SP1 Redistributable
  - Java Runtime Environment (JRE) 1.7.0_06
  - Tomcat 7.0.29

Binärdateien mit unrichtigen Informationen zur Dateiversion

CA ARCserve Central Applications installiert Binärdaten von Drittanbietern, aus anderen CA-Produkten und aus CA ARCserve Central Applications, die unrichtige Informationen zur Dateiversion enthalten. In der folgenden Tabelle werden diese Binärdaten beschrieben.

Binärname	Quelle
UpdateData.exe	CA License
zlib1.dll	Zlib Compression Library

Binärdateien ohne eingebettetes Manifest

CA ARCserve Central Applications installiert Binärdaten von Drittanbietern, aus anderen CA Technologies-Produkten und aus CA ARCserve Central Applications, die kein eingebettetes Manifest und kein Text-Manifest enthalten. In der folgenden Tabelle werden diese Binärdaten beschrieben.

Binärname	Quelle
BaseLicInst.exe	CA License
UpdateData.exe	CA License
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
tomcat7.exe	Tomcat

Binärdateien mit "Require Administrator"-Berechtigungen im Manifest

CA ARCserve Central Applications installiert Binärdaten von Drittanbietern, aus anderen CA Technologies-Produkten und aus CA ARCserve Central Applications, die über die Berechtigungsebene "Administrator" oder "Highest Available" verfügen. Sie müssen sich mit einem Administratorkonto oder einem Konto mit den höchstmöglichen Berechtigungen anmelden, um verschiedene Dienste, Komponenten und Anwendungen von CA ARCserve Central Applications ausführen zu können. Die Binärdateien für diese Dienste, Komponenten und Anwendungen enthalten CA ARCserve Central Applications-spezifische Funktionen, die für ein normales Benutzerkonto nicht verfügbar sind. Daher werden Sie von Windows aufgefordert, einen Vorgang zu bestätigen, indem Sie Ihr Kennwort angeben oder ein Konto mit Administratorrechten verwenden, um den Vorgang auszuführen.

- **Administratorrechte** - Das Administratorprofil sowie Konten mit Administratorrechten verfügen über Schreib-, Lese- und Ausführungsberechtigungen für alle Windows- und Systemressourcen. Wenn Sie über keine Administratorrechte verfügen, werden Sie aufgefordert, den Benutzernamen und das Kennwort eines Administrators einzugeben, um fortfahren zu können.
- **Höchstmögliche Berechtigungen** - Bei einem Konto mit den höchst möglichen Berechtigungen handelt es sich um ein normales Benutzerkonto oder Poweruser-Konto, mit dem Administratorrechte genutzt werden können.

In der folgenden Tabelle werden diese Binärdaten beschrieben.

Binärname	Quelle
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications

Binärname	Quelle
RemoteDeploy.exe	CA ARCserve Central Applications
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Ausschließen von Dateien vom Antivirusscanning

Antivirus-Software kann die reibungslose Ausführung der Anwendung behindern, indem sie entweder zeitweilig den Zugriff auf Dateien blockiert, oder indem Sie Dateien in Quarantäne stellt oder löscht, die fälschlicherweise als verdächtig oder gefährlich klassifiziert werden. Sie können die meiste Antivirus-Software so konfigurieren, dass bestimmte Prozesse, Dateien oder Ordner ausgeschlossen werden, damit Sie keine Daten durchsuchen, die nicht geschützt werden müssen. Es ist wichtig, Ihre Antivirus-Software richtig zu konfigurieren, damit sie keine Sicherungs- und Wiederherstellungsvorgänge oder andere Prozessarten behindert.

Die folgenden Prozesse, Ordner und Dateien sollten aus dem Antivirusscanning ausgeschlossen werden:

- Prozessliste
  - C:\Programme\CA\ARCserve Central Applications\BIN\CCIConfigSettings.exe
  - C:\Programme\CA\ARCserve Central Applications\BIN\CfgUpdateUtil.exe
  - C:\Programme\CA\ARCserve Central Applications\BIN\DBConfig.exe
  - C:\Programme\CA\ARCserve Central Applications\BIN\GetApplicationDetails.exe
  - C:\Programme\CA\ARCserve Central Applications\BIN\GetApplicationDetails64.exe
  - C:\Programme\CA\ARCserve Central Applications\BIN\GetVolumeDetails.exe
  - C:\Programme\CA\ARCserve Central Applications\BIN\VixGetApplicationDetails.exe
  - C:\Programme\CA\ARCserve Central Applications\BIN\VixGetVolumeDetails.exe
  - C:\Programme\CA\ARCserve Central Applications\BIN\GetApplicationDetails64.exe
  - C:\Programme\CA\ARCserve Central Applications\Deployment\Asremsvc.exe
  - C:\Programme\CA\ARCserve Central Applications\Deployment\CheckProdInfo.exe
  - C:\Programme\CA\ARCserve Central Applications\Deployment\DeleteMe.exe
  - C:\Programme\CA\ARCserve Central Applications\Deployment\SetupComm.exe
  - C:\Programme\CA\ARCserve Central Applications\Deployment\RestartHost.exe
  - C:\Programme\CA\ARCserve Central Applications\Update Manager\D2DAutoUpdateUninstallUtility.exe
  - C:\Programme\CA\ARCserve Central Applications\Update Manager\D2DPMConfigSettings.exe

- C:\Programme\CA\ARCserve Central Applications\Update Manager\D2DUpdateManager.exe
- C:\Programme\CA\ARCserve Central Applications\Update Manager\UpgradeDataSyncupUtility.exe
- C:\Programme\CA\ARCserve Central Applications\TOMCAT\BIN\tomcat7.exe
- C:\Programme\CA\ARCserve D2D\TOMCAT\JRE\jre7\bin
  - java.exe
  - java-rmi.exe
  - javaw.exe
  - keytool.exe
  - rmid.exe
  - rmiregistry.exe
- C:\Programme (x86)\CA\SharedComponents\CA_LIC
  - CALicnse.exe
  - CAminfo.exe
  - CAregit.exe
  - ErrBox.exe
  - lic98log.exe
  - lic98Service.exe
  - lic98version.exe
  - LicDebug.exe
  - LicRCmd.exe
  - LogWatNT.exe
  - mergecalic.exe
  - mergeolf.exe

Terminologieglossar

Auto-Discovery

Auto-Discovery ist ein Prozess, bei dem Knoten entdeckt und zu einer oder mehreren CA ARCserve Central Applications für zentrale Verwaltung hinzugefügt werden.

HOTADD-Transportmodus

Der Hotadd-Transportmodus ist eine Methode zum Datentransport, mit der Sie mit SCSI-Datenträgern konfigurierte virtuelle Rechner sichern können. Weitere Informationen finden Sie im "Virtual Disk API Programming Guide" auf der VMware-Website.

Katalogdatei

Eine Katalogdatei ist ein Verzeichnis mit Informationen zu den Sicherungsdaten in der CA ARCserve D2D-Datenbank. Weitere Informationen zur CA ARCserve D2D-Katalogdatei finden Sie im *CA ARCserve D2D-Benutzerhandbuch.*

Knoten

Ein Knoten ist ein physischer oder virtueller Rechner, der über einen oder mehrere CA ARCserve Central Applications verwaltet wird.

Knotengruppe

Eine Knotengruppe ist eine Methode, bei der alle Knoten, die über eine oder mehrere CA ARCserve Central Applications verwaltet werden, organisiert werden können, wie beispielsweise nach Zweck, Betriebssystem oder nach installierten Anwendungen.

NBDSSL-Transportmodus

Der Transportmodus für Network Block Device Secure Sockets Layer (NBDSSL) verwendet das NFC-Protokoll (Network File Copy) zur Kommunikation. NBDSSL-Übertragungen verschlüsseln Daten mithilfe des TCP/IP-Kommunikationsnetzwerks.

NBD-Transportmodus

Der NBD-Transportmodus (Network Block Device), auch LAN-Transportmodus genannt, verwendet das NFC-Protokoll (Network File Copy) zum Kommunizieren. Verschiedene VDDK- und VCB-Vorgänge verwenden eine Verbindung für jeden virtuellen Datenträger, auf den bei der Verwendung von NBD auf jedem ESX-/ESXi-Server-Host zugegriffen wird.

Preflight-Check

"Preflight-Check" (PFC) ist ein Hilfsprogramm, das Sie entscheidende Überprüfungen auf Knoten ausführen lässt, um Bedingungen zu erkennen, die Sicherungsjobs fehlschlagen lassen können. Sie können die Ergebnisse des PFC für einen Knoten anzeigen, indem Sie auf das Symbol in der Spalte "PFC-Status" auf dem Fenster "Knoten" klicken.

Richtlinie

Eine Richtlinie ist eine Gruppe von Spezifikationen, um einen Knotens in einer oder mehreren CA ARCserve Central Applications zu schützen.

SAN-Transportmodus

Der SAN-Transportmodus (Storage Area Network) ermöglicht es Ihnen, Sicherungsdaten von Proxy-Systemen, die mit SAN verbunden sind, mithilfe von FibreChannel-Kommunikation in Speichergeräte zu übertragen.

Sicherungs-Proxy

Ein Sicherungs-Proxy ist der Host-Computer, auf dem CA ARCserve D2D ausgeführt wird. Der Proxy führt die Sicherungsvorgänge aus, die in CA ARCserve Central Host-Based VM Backup konfiguriert wurden.

SRM

Storage Resource Management (SRM) ist eine Funktion, bei der Informationen gesammelt werden, um Ihre Umgebung, wie beispielsweise Anwendungsdaten, Hardware- und Software-Daten oder Leistungsschlüsselindikator, effektiv verwalten zu können.

Synchronisierung

Synchronisierung ist der Prozess, bei dem Daten in verschiedenen Datenbanken auf dem neuesten Stand gehalten werden, sodass die Datenbank des zentralen Servers konsistent mit registrierten Zweigstellen, Knoten oder Standorten ist.

Wiederherstellungspunkt

Ein Wiederherstellungspunkt ist ein Sicherungs-Image, das übergeordnete und die ältesten untergeordneten Blöcke umfasst. Untergeordnete Sicherungen werden mit der übergeordneten Sicherung zusammengeführt, um neue Wiederherstellungspunkt-Images zu erstellen, sodass der angegebene Wert immer verwaltet wird.